A Min-max Optimization-based Approach for Secure Localization in Wireless Networks

Slavisa Tomic and Marko Beko

***Abstract*—Range-based localization of a target device in wireless networks in the presence of malicious attackers that tend to disrupt the localization process by counterfeiting (spoofing) their radio measurements is addressed in this work. In contrast to state-of-the-art methods, that assume that all devices participating in the process are non-malicious in the beginning, we here tackle the problem from the opposite perspective. All devices are treated as malicious at first, and, by assuming that an upper-bound on the attack intensity is (imperfectly) known a priori, the worst-case scenario is studied, from which two novel estimators are derived. The first approach is based on convex relaxation and leads to a robust second-order cone programming (R-SOCP), while the other one assumes problem reformulation as a robust generalized trust region sub-problem (R-GTRS). Received signal strength (RSS) scenario is in the main focus, but an adaptation of the new approach to a general range-based setting is presented as well. The proposed min-max approach is validated though computer simulations, where it showed its worthiness by outperforming the state-of-the-art approaches and offering a more reliable (secure) solution to the problem. Finally, it is worth mentioning that a theoretical analysis on the detection performance is also included in the work.**

***Index Terms*—Convex optimization, distance-spoofing, generalized trust region sub-problem (GTRS), min-max approach, probability of detection, robust localization, second-order cone programming (SOCP), secure localization.**

I. Introduction

Accurate determination of object's location (e.g., a wireless device) plays a paramount role in many applications such as in positioning, tracking and autonomous navigation systems [1], [2]. Nevertheless, the majority of currently available location-based services (such as [3]-[6]) are vulnerable to security threats [7], since malicious agents (attackers) can easily access the network and disable accurate localization process (for instance, either by impersonating genuine devices or by modifying their code to turn them malicious). Moreover, in many situations, it suffices to simply obstruct a direct wireless link between two genuine devices to aggravate the localization process, since this leads to reduced power of the received signal, corresponding to increased distance estimation. Note that in these cases, the adversary does not even need to break any crypto, nor expose to risk of breaking any upper layer protocols when setting the malicious deed [8], [9]. Besides, inadvertent errors (malfunctions) can occur at any time. Therefore, simply localizing an object might not be sufficient in many applications nowadays, but localization must be done securely in order to avoid calamities or even fatal outcomes.

The authors in [8] and [9] proposed a secure-ranging solution, but their main goal was to study design of schemes to ratify that the distance between two devices is as it is proclaimed. To accomplish this, both works employed bounding protocols, like verifiable multilateration and location verification, to endure attacks [8], [9].

Over the last years, several secure localization systems have been developed [10]-[20]. The work in [10], proposed a greedy approach to determine the location consistent with the largest number of measurements from reference points. In [10], the authors divided the localization area into a grid and presented a voting-based scheme with the goal to count the votes of a grid point based on established criteria. The authors in [11] designed an attack-resistant and device-independent method based on Petri-net. In [12], an iterative gradient descent approach employing discrepant observation trimming to remove the devices with large residues from the localization process based on iterative updating of the cost function was proposed. A couple of solutions that are based on spatial-density clustering to distinguish atypical groups was proposed in [13]. To prevent introducing local outliers into normal groups, an adjustable clustering algorithm was carried out, after which a sequential probability ratio test founded on consistency properties of both time of arrival (TOA) and received signal strength (RSS) observations was implemented to improve detection performance. The work in [14] introduced two classes of attacks (aligned node location and inside-attack) in which the attackers employ their own knowledge about the target location. In the former one, collinearity of devices is exploited, whereas in the latter one degree of consistency filtering debilitation algorithm is used by placing malicious devices within benign ones. The work proposed a solution relying on a novel beacon placement strategy together with a filtering technique that filters-out malicious location references launched by inside-attacks. The authors in [15] proposed a device identification algorithm based on the reverse time synchronization strategy where devices' clock skews are determined at the head of a wireless network and the spatially-correlated radio link information to accomplish simultaneous device identification and attack detection. The work in [16], introduced a weighted least squares (WLS) estimator for RSS-based localization, under non-cryptographic uncoordinated at-

This research was partially funded by Fundação para a Ciência e a Tecnologia under Projects UIDB/04111/2020, UIDB/50008/2020, ROBUST EXPL/EEI-EEE/0776/2021, and 2021.04180.CEECIND, and by the European Union's Horizon Europe Research and Innovation Programme under the Marie Skłodowska-Curie grant agreement No. 101086387.

S. Tomic is with COPELABS, Universidade Lusófona, Campo Grande 376, 1749 - 024 Lisboa, Portugal. (e-mail: slavisa.tomic@ulusofona.pt). M. Beko is with Instituto de Telecomunicações, Instituto Superior Técnico, Universidade de Lisboa, 1049-001 Lisbon, Portugal (e-mail: marko.beko@tecnico.ulisboa.pt) and also with COPELABS, Universidade Lusófona, Campo Grande 376, 1749 - 024 Lisboa, Portugal.

tacks. The proposed WLS estimator was derived by defining an opportune weight allocation based on log-distance model, where *remote* devices receive small weights and vice versa. In the work of [17], the authors considered sequential localization (tracking) problem of a moving device in mobile IoT networks in the presence of malicious attackers. Based on some particular assumptions on prior distributions on attack parameters and uncertainties, the authors in [17] formulated the tracking problem as a maximum a posteriori one, and solved it by employing an iterative variational message passing-based algorithm that approximates the intractable posterior probability by the product of variational distributions. Finally, the identification of malicious nodes came as a byproduct of the obtained solution. In [18], another clustering scheme based on circle intersections followed by a threshold-based keying process was proposed to detect attackers, which are then omitted from a non-linear localization process transformed into a generalized trust region sub-problem (GTRS) framework. The authors in [18] assumed that an attacker can only enlarge distance measurements by considering the use of two-way TOA measurements.

Very recently, both works of [16] and [18] were resumed and updated by the introduction of a new secure WLS (SWLS) [19] for RSS-based localization and the consideration of a general range-based measurement technique and the use of law of cosines (LC) for the derivation of a novel LC-GTRS scheme [20], respectively. It is worth mentioning that the SWLS method [19] relies on the exact knowledge of the noise power and empirical tuning of a hyperparameter to establish a threshold and distinguish between malicious and non-malicious devices, while the LC-GTRS method in [20] requires that the difference between non-malicious and malicious devices is at least three (in a 2-dimensional space).

Unlike the state-of-the-art methods, that consider all devices as non-malicious at first, this work contemplates the problem from a different perspective. From the very beginning, the worst-case scenario is of interest and all devices are considered as malicious at first. By assuming that the upper-bound of the magnitude of the attack intensity is (imperfectly) known beforehand, the malicious attacks are treated as nuisance parameters after which a min-max approach is applied to formulate the secure localization problem as a robust non-linear least squares estimator. Two approaches are then proposed: one based on second-order cone relaxation to convert the non-linear problem into a convex robust second-order cone programming (R-SOCP) problem, and another one based on a weighting strategy and approximation to cast the problem into a robust GTRS (R-GTRS) framework. The former one can be readily solved by convex optimization tools, such as CVX [21], while the latter one is suitable for solving via bisection [22].

The main contributions of the present work are four-fold, and are summarized as follows:

- This work proposes a novel perspective on the localization problem in the presence of malicious attackers/malfunctions, where all devices are considered as malicious at first in order to study the worst-case scenario.
- It formulates the secure localization problem in the form of a robust non-linear least squares estimator by applying a min-max approach and treating the malicious attacks as nuisance parameters, assuming that the upper-bound on the magnitude of the attack intensity is (imperfectly) known.
- The current work introduces two robust estimators to solve the secure localization problem via second-order cone relaxation technique, and a weighting strategy and GTRS framework.
- Based on the minimum probability of error criterion, the work proposes a novel maximum (conditional) likelihood detector in closed-form (both theoretical and practical), where the conditional likelihood ratio is compared to a threshold in order to detect malicious attackers.

II. Problem Formulation

Consider an arbitrarily deployed 2-dimensional[1] wireless network containing a target node whose unknown location (that we wish to estimate) is represented by $\boldsymbol{x}$ and N stationary reference nodes (anchors) whose true (known) locations are represented by $\boldsymbol{a}_i$, $i = 1, ..., N$. We assume that the target can *hear* all reference points, and that it is opportunely equipped in order to withdraw distance measurements from the received radio signal (e.g., via TOA or RSS measurements). Furthermore, we assume that some portion (anywhere from none to all) of the reference points are malicious or damaged, so that their measurements incline to hinder the localization process. These malicious strikes (or possibly failures) include counterfeiting their own distance observations (for instance, by changing the transmit power levels), and are assumed uncoordinated (all attackers operate independently from each other) and non-cryptographic (no risk of upper-layer security protocol violations when realizing attacks). Therefore, by assuming that the signal power is dominated by path loss (which can be modeled using the log-distance model [23]), the k-th RSS measurement sample ($1 \leq k \leq K$) between the target node and the i-th reference point (in dBm) is modeled as

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

where P_0 denotes the received power at a reference distance d_0 (usually, $d_0 = 1$ m), γ is the path loss exponent, $n_{i,k}$ represents the measurement noise, modeled as a zero-mean Gaussian random variable, i.e., $n_{i,k} \sim \mathcal{N}(0, \sigma_{i,k}^2)$, and $\delta_i \in \mathbb{R}$ is the (unknown) intensity of the spoofing attack ($\delta_i = 0$ if the reference point i is not malicious). Note that this work does not make any assumptions about the distribution of the spoofing attacks; it only requires that the magnitude of the attack intensity is (imperfectly) upper bounded by a constant, i.e., $|\delta_i| \leq \Delta$, for $i = 1, ..., N$. This is a mild assumption, since in practice the value of Δ could be determined by physical limitations of the environment and/or hardware employed (for instance, by knowing the size of the area of interest, communication range, receiver sensibility, etc.). Besides, an attacker cannot perform unlimited distance reduction attacks (since distance cannot take on negative values), while exaggeration in

[1]The generalization of the proposed solutions to a 3-dimensional scenario is straightforward.

distance enlargement attacks would most likely easily expose the attacker, since it would make difficult for an attacker to hide its malicious intentions within noise [18]. In the following text, the median of the K RSS measurements, P_i, is calculated for each link i and is used for the sake of simplicity. Likewise, with the goal of simplifying the notation and with no loss of generality, the measurement variances are considered equal for any link i (and sample k), i.e., $\sigma_1^2 = \sigma_2^2 = \ldots = \sigma_N^2 = \sigma^2$.

Following the maximum likelihood (ML) criterion [24, Ch. 7] and exploiting the RSS observation in (1), the target location can be determined as

$$\widehat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x}} \sum_{i=1}^{N} \frac{1}{\sigma_i^2} \left(P_0 - P_i - \delta_i - 10\gamma \log_{10} \frac{\|\boldsymbol{x} - \boldsymbol{a}_i\|}{d_0} \right)^2. \tag{2}$$

The ML estimator is among the most commonly used estimators in practice, owing to its asymptotically optimal performance (when large enough data records are available) [24, Ch. 7]. Still, the problem in (2) is under-determined and difficult to tackle directly, since it is highly non-convex. Hence, a new approach is proposed in the following section, which allows for efficient circumvention of the non-convexity in (2), resulting in two robust solutions.

III. The Proposed Robust Approach

Unlike the existing approaches that first consider all reference points as honest in order to detect attackers, a different approach is taken here, in which all reference points are considered as malicious from the start, i.e., the worst-case scenario is studied. In this regard, start by adding $\frac{\Delta}{2}$ to both sides of (1) to get

$$\rho_i 10^{\frac{n_i}{10\gamma}} = \lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|, \tag{3}$$

where $\rho_i = d_0 10^{\frac{P_0 - \tilde{\delta}_i}{10\gamma}}$ and $\lambda_i = 10^{\frac{P_i + \Delta/2}{10\gamma}}$, with $\tilde{\delta}_i = \delta - \frac{\Delta}{2}$. By applying the first-order Taylor-series expansion to $10^{\frac{n_i}{10\gamma}}$, (3) can be approximated by

$$\rho_i \left(1 + \frac{\ln(10)}{10\gamma} n_i \right) \approx \lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|.$$

Rearranging and squaring the above expression, yields

$$\rho_i^2 \approx \lambda_i^2 \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - 2\epsilon_i \lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\| + \epsilon_i^2,$$

where $\epsilon_i \sim \mathcal{N}\left(0, \left(\rho_i \frac{\ln(10)}{10\gamma} \sigma_i\right)^2\right)$. Loosely speaking, by disregarding the second-order noise term, from the above expression one gets

$$\epsilon_i \approx \frac{\lambda_i^2 \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \rho_i^2}{2\lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|}, \tag{4}$$

Motivated by the desire to analyze the worst-case scenario, the following min-max problem is derived from (4):

$$\underset{\boldsymbol{x}}{\text{minimize}} \ \underset{\rho_i}{\text{maximize}} \sum_{i=1}^{N} \left(\frac{\lambda_i^2 \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \rho_i^2}{2\lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|} \right)^2. \tag{5}$$

By defining $f(\rho_i) = \frac{\left|\lambda_i^2 \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \rho_i^2\right|}{2\lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|}$, the problem in (5) becomes equivalent to

$$\underset{\boldsymbol{x}}{\text{minimize}} \ \underset{\rho_i}{\text{maximize}} \sum_{i=1}^{N} f(\rho_i)^2.$$

Moreover, since

$$\underset{\rho_i}{\text{maximize}} \sum_{i=1}^{N} f(\rho_i)^2 = \sum_{i=1}^{N} \left[\underset{\rho_i}{\text{maximize}} \, f(\rho_i) \right]^2,$$

and, by definition

$$|\rho_i| = \left| \delta_i - \frac{\Delta}{2} \right| \leq \frac{\Delta}{2},$$

it follows that

$$\underset{\rho_i}{\text{maximize}} f(\rho_i) = \begin{cases} f\left(-\frac{\Delta}{2}\right), & \text{if } f\left(-\frac{\Delta}{2}\right) \geq f\left(\frac{\Delta}{2}\right) \\ f\left(\frac{\Delta}{2}\right), & \text{if } f\left(-\frac{\Delta}{2}\right) < f\left(\frac{\Delta}{2}\right) \end{cases},$$

with

$$f\left(-\frac{\Delta}{2}\right) = \frac{\left|\lambda_i^2 \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \eta^2\right|}{2\lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|},$$

$$f\left(\frac{\Delta}{2}\right) = \frac{\left|\lambda_i^2 \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \nu^2\right|}{2\lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|},$$

and $\eta = d_0 10^{\frac{P_0 + \Delta/2}{10\gamma}}$ and $\nu = d_0 10^{\frac{P_0 - \Delta/2}{10\gamma}}$.

Finally, bearing in mind that $\max\{\alpha, \beta\} \leq \alpha + \beta$ for some $\alpha, \beta \geq 0$, one can circumvent tackling (5) directly, and minimize its upper bound instead, i.e.,

$$\begin{aligned} \underset{\boldsymbol{x}}{\text{minimize}} & \sum_{i=1}^{N} \left(\frac{\lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \lambda_i^{-1} \eta^2}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|} \right)^2 \\ & + \sum_{i=1}^{N} \left(\frac{\lambda_i \|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \lambda_i^{-1} \nu^2}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|} \right)^2. \end{aligned} \tag{6}$$

Due to the norm terms (in both numerators and denominators), the least squares problem in (6) is non-linear; thus, it is still difficult to solve it directly. Nonetheless, in the following two subsections we show how to convert (6) into (robust) SOCP and GTRS frameworks respectively, which can be readily solved by convex optimization and bisection tools, respectively, followed by an analysis on attacker detection.

A. The Proposed R-SOCP estimator

One can convert the non-convex problem in (6) into a convex one by resorting to second-order cone relaxation (SOCR) technique. To this end, develop the square-norm terms in the numerators and introduce an auxiliary variable $y = \|\boldsymbol{x}\|^2$, together with epigraph variables $\boldsymbol{e} = [e_i]^T \in \mathbb{R}^N$ and $\boldsymbol{t} = [t_i]^T \in \mathbb{R}^N$, with e_i and t_i corresponding to the i-th factors of the two sums in the objective function, respectively. Enforce SOCR technique to *convexify* $y = \|\boldsymbol{x}\|^2$ as $y \geq \|\boldsymbol{x}\|^2$, as well as on the constraints involving the epigraph variables of the form $s = \left(\frac{r}{c}\right)^2$ as $s \geq \left(\frac{r}{c}\right)^2$. The problem in (6) is then relaxed into the following SOCP problem [25, Ch. 4].

$$\underset{\boldsymbol{x}, y, \boldsymbol{e}, \boldsymbol{t}}{\text{minimize}} \ \mathbf{1}_{1\times N} \boldsymbol{e} + \mathbf{1}_{1\times N} \boldsymbol{t} \tag{7a}$$

subject to

$$\left\| \begin{bmatrix} 2\boldsymbol{x} \\ y-1 \end{bmatrix} \right\| \leq y+1, \tag{7b}$$

$$\begin{aligned} &\left\| \begin{bmatrix} 2\left(\lambda_i\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-\lambda_i^{-1}\eta^2\right) \\ 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-e_i \end{bmatrix} \right\| \\ &\leq 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)+e_i, \;\; i=1,...,N, \end{aligned} \tag{7c}$$

$$\begin{aligned} &\left\| \begin{bmatrix} 2\left(\lambda_i\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-\lambda_i^{-1}\nu^2\right) \\ 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-t_i \end{bmatrix} \right\| \\ &\leq 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)+t_i, \;\; i=1,...,N, \end{aligned} \tag{7d}$$

where the constraints of the form $s \geq \left(\frac{r}{c}\right)^2$ are written in a more usual conic form, $\|[2r; c^2-s]\| \leq c^2+s$. The estimator in (7) can be readily solved by convex optimization tools such as CVX [21], and is denoted by "R-SOCP" in the remaining text.

An important issue one has to consider is feasibility and sensitivity of the solution of (7) to perturbations in model parameters. These properties are difficult to address for (7) directly, since it is not strongly convex. Nevertheless, one can readily obtain a strongly convex version of (7) by adding a quadratic penalty term with an arbitrarily-small regularization parameter (e.g., $\epsilon = 10^{-32}$) into the objective function. More precisely, a strongly convex counterpart of (7) can be written as

$$\underset{\boldsymbol{x},y,\boldsymbol{e},\boldsymbol{t}}{\text{minimize}} \; \mathbf{1}_{1\times N}\boldsymbol{e}+\mathbf{1}_{1\times N}\boldsymbol{t}+\epsilon\|[\boldsymbol{x}^T,y,\boldsymbol{e}^T,\boldsymbol{t}^T]^T\|^2 \tag{8a}$$

subject to (8b) = (7b), (8c) = (7c) and (8d) = (7d).

From the practical/engineering point of view, the two problems are virtually identical, but the latter one is strongly convex, meaning that it has a unique solution (given that it exists). Moreover, one can easily see that the feasible set of solutions for (8), defined by the $2N+3$-tuple as

$$\begin{aligned} \mathcal{F} = \big\{ &(\boldsymbol{x}, y, e_1, ..., e_N, t_1, ..., t_N) : y \geq \|\boldsymbol{x}\|^2, \\ &e_i \geq \frac{\left(2\left(\lambda_i\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-\frac{\eta^2}{\lambda_i}\right)\right)^2}{16\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)}, \\ &t_i \geq \frac{\left(2\left(\lambda_i\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-\frac{\nu^2}{\lambda_i}\right)\right)^2}{16\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)}, \\ &i=1,...,N\big\}, \end{aligned}$$

where the inequalities that involve e_i and t_i are derived directly from (7c) and (7d) (i.e., (8c) and (8d)) respectively, is closed. Note that $\mathcal{F}$ is also non-empty, given that the point ($\boldsymbol{x} = [0,0]^T, y=0$) is always feasible. This can be seen by plugging this point into (7c) (i.e., (8c)) which boils down to

$$\sqrt{(2\lambda_i\|\boldsymbol{a}_i\|^2-2\lambda_i^{-1}\eta^2)^2+(4\|\boldsymbol{a}_i\|^2-e_i)^2} \leq 4\|\boldsymbol{a}_i\|^2+e_i.$$

After squaring both sides and applying simple algebraic manipulations, the above expression is equivalent to

$$e_i \geq \frac{(2\lambda_i\|\boldsymbol{a}_i\|^2-2\lambda_i^{-1}\eta^2)^2}{16\|\boldsymbol{a}_i\|^2}.$$

Obviously, similar can be done for the constraint in (7d) (i.e., 8d). Thus, it suffices to choose e_i and t_i sufficiently large in order for $\mathcal{F}$ to be non-empty. Therefore, we can conclude that the problem is always feasible. Moreover, it can be shown that the solution map of (8) is continuous. The proof is omitted here due to space limitations.

B. The Proposed R-GTRS estimator

In the convex optimization sense, the main troublemakers in (6) are the norm terms in the denominators. Nevertheless, since these are actually distances between the target and the reference points, they can be simply substituted by their respective ML estimates, $\widehat{d}_i = d_0 10^{\frac{P_0-P_i}{10\gamma}}$. Furthermore, with the aim of reducing the significance of reference points that produce *remote* distances to the target, define weights, $w_i = \frac{10^{\frac{P_i}{10}}}{\sum_{i=1}^N 10^{\frac{P_i}{10}}}$ (note that P_i is given in dBm; hence, the measurements are converted to mW), to obtain

$$\begin{aligned} \underset{\boldsymbol{x}}{\text{minimize}} &\sum_{i=1}^N w_i\left(\frac{\lambda_i\|\boldsymbol{x}-\boldsymbol{a}_i\|^2-\lambda_i^{-1}\eta^2}{2\widehat{d}_i}\right)^2 \\ &+\sum_{i=1}^N w_i\left(\frac{\lambda_i\|\boldsymbol{x}-\boldsymbol{a}_i\|^2-\lambda_i^{-1}\nu^2}{2\widehat{d}_i}\right)^2, \end{aligned}$$

which, after expanding the square terms and disregarding the denominator (which has no effect on the minimization now), can be written in the vector form as

$$\underset{\boldsymbol{y}=[\boldsymbol{x},\,\|\boldsymbol{x}\|^2]^T}{\text{minimize}} \left\{ \|\boldsymbol{H}\boldsymbol{y}-\boldsymbol{h}\|^2 : \;\; \boldsymbol{y}^T\boldsymbol{B}\boldsymbol{y}+2\boldsymbol{b}^T\boldsymbol{y}=0 \right\}, \tag{9}$$

where $\boldsymbol{H} \in \mathbb{R}^{2N\times 3}$ and $\boldsymbol{h} \in \mathbb{R}^{2N}$ are given by

$$\boldsymbol{H} = \boldsymbol{W}\begin{bmatrix} \vdots & \vdots \\ 2\lambda_i\boldsymbol{a}_i^T & -\lambda_i \\ \vdots & \vdots \\ 2\lambda_i\boldsymbol{a}_i^T & -\lambda_i \\ \vdots & \vdots \end{bmatrix}, \;\; \boldsymbol{h} = \boldsymbol{W}\begin{bmatrix} \vdots \\ \lambda_i\|\boldsymbol{a}_i\|^2-\lambda_i^{-1}\eta^2 \\ \vdots \\ \lambda_i\|\boldsymbol{a}_i\|^2-\lambda_i^{-1}\nu^2 \\ \vdots \end{bmatrix},$$

$$\boldsymbol{B} = \begin{bmatrix} \boldsymbol{I}_2 & \mathbf{0}_{2\times 1} \\ \mathbf{0}_{1\times 2} & 0 \end{bmatrix} \in \mathbb{R}^{3\times 3}, \; \boldsymbol{b} = \begin{bmatrix} \mathbf{0}_{2\times 1} \\ -0.5 \end{bmatrix} \in \mathbb{R}^3,$$

with $\boldsymbol{W} = \text{diag}\left(\left[..., \sqrt{w_i}, ..., \sqrt{w_i}, ...\right]^T\right) \in \mathbb{R}^{2N\times 2N}$, and $\boldsymbol{I}_q$ and $\mathbf{0}_{v\times u}$ denoting the identity matrix of size q and the matrix of all-zero entries of size $v \times u$. Notice that both the objective function and the constraint in (9) are quadratic with respect to the optimization variable $\boldsymbol{y}$. This class of optimization problems is referred to as GTRS in the literature, and its *exact* solution can be obtained by a bisection procedure, since there is a readily computable interval on which GTRS is a monotonically decreasing function [22], [26]. The estimator in (9) is denoted by "R-GTRS" in the remaining text[2].

[2]Note that the SWLS method in [19] is designed for RSS-based localization originally. Since its derivation is based on a non-linear relationship between the RSS and the distance (where positive and negative variations in the RSS are exploited), its generalization to a common range-based setting (e.g., TOA) is not straightforward. Therefore, this work opts to consider RSS setting mainly, but it also provides a generalization of the proposed approach to a common range-based scenario in Appendix A.

C. Attacker Detection

On the one hand, in the considered problem (where even all reference points could be attackers simultaneously) it is reasonable to express an even prior belief in the likelihood of the following hypotheses: $\mathcal{H}_0$ (reference node is not malicious) and $\mathcal{H}_1$ (reference node is malicious), i.e., $P(\mathcal{H}_0) = P(\mathcal{H}_1) = 1/2$, where $P(\mathcal{H}_0)$ and $P(\mathcal{H}_1)$ are the prior probabilities of the respective hypotheses. On the other hand, since the malicious attacker is equally likely to enlarge or reduce the received strength, one has that $P(\mathcal{H}_1) = P(\mathcal{H}_{10}) + P(\mathcal{H}_{11})$, with $\mathcal{H}_{10}$ and $\mathcal{H}_{11}$ denoting respectively the prior hypotheses of a negative and positive attack carried out by an attacker. This approach of assigning prior probabilities is known as the Bayesian approach to hypothesis testing [27, Ch. 3].

In order to maximize the probability of (correct) detection, one needs to derive a test statistic. This can be done by maximizing the conditional probability density function for each link i

$$p(\boldsymbol{\theta}_i|\mathcal{H}_j) = \frac{1}{(\sqrt{2\pi\sigma^2})^{\frac{K}{2}}} \exp\left\{-\frac{1}{2\sigma^2}\sum_{k=1}^{K}\left(\theta_{i,k} - A_j\right)^2\right\}, \tag{10}$$

for $j = 0, 1$, where $\boldsymbol{\theta}_i = \left[\theta_{i,k}\right]^T$, $\theta_{i,k} = P_0 - P_{i,k} - 10\gamma\log_{10}\frac{\|\boldsymbol{x}-\boldsymbol{a}_i\|}{d_0}$, $A_0 = 0$, and $A_1 = \delta_i$. Maximizing (10) is equivalent to minimizing

$$\begin{aligned}\sum_{k=1}^{K}\left(\theta_{i,k} - A_j\right)^2 &= \sum_{k=1}^{K}\left(\theta_{i,k} - \bar{\theta}_i + \bar{\theta}_i - A_j\right)^2 \\ &= \sum_{k=1}^{K}\left(\theta_{i,k} - \bar{\theta}_i\right)^2 + K\left(\bar{\theta}_i - A_j\right)^2,\end{aligned} \tag{11}$$

with $\bar{\theta}_i$ being the mean value of $\boldsymbol{\theta}_i$. Therefore, it is clear that in order to minimize (11) one has to choose $\mathcal{H}_j$ for which A_j is the closest to $\bar{\theta}_i$, i.e., one should decide

$$\begin{aligned}\mathcal{H}_0, &\quad \text{if } \left|\bar{\theta}_i\right| < \tfrac{\delta_i}{2}, \\ \mathcal{H}_1, &\quad \text{if } \left|\bar{\theta}_i\right| > \tfrac{\delta_i}{2}.\end{aligned}$$

According to the Bayesian paradigm the (theoretical) probability of (correct) detection is determined as

$$\begin{aligned}P_D &= \sum_{j=0}^{1} P(\mathcal{H}_j|\mathcal{H}_j)P(\mathcal{H}_j) = \frac{1}{2}\text{Pr}\{-\frac{\delta_i}{2} < \bar{\theta}_i < \frac{\delta_i}{2}|\mathcal{H}_0\} \\ &+\tfrac{1}{4}\left[\text{Pr}\{\bar{\theta}_i < -\tfrac{\delta_i}{2}|\mathcal{H}_{10}\} + \text{Pr}\{\bar{\theta}_i > \tfrac{\delta_i}{2}|\mathcal{H}_{11}\}\right],\end{aligned}$$

where $P(U|V)$ is the conditional probability that indicates the probability of detecting U when V is true. Since, conditioned on $\mathcal{H}_j$, one has that $\bar{\theta}_i \sim \mathcal{N}(A_j, \frac{\sigma^2}{K})$, the probability of detection [27, Ch. 3] is given by

$$\begin{aligned}P_D &= \tfrac{1}{2}\left[1 - Q\left(\frac{-\delta_i/2}{\sqrt{\sigma^2/K}}\right) - Q\left(\frac{\delta_i/2}{\sqrt{\sigma^2/K}}\right)\right] \\ &+\tfrac{1}{4}\left[1 - Q\left(\frac{-\delta_i/2+\delta_i}{\sqrt{\sigma^2/K}}\right) - Q\left(\frac{\delta_i/2-\delta_i}{\sqrt{\sigma^2/K}}\right)\right] \\ &= 1 - \tfrac{3}{2}Q\left(\sqrt{\frac{K\delta_i^2}{4\sigma^2}}\right).\end{aligned} \tag{12}$$

Note that the true information about δ_i and σ required to calculate P_D is not available beforehand in practice. Hence, the result in (12) is used as a (theoretical) benchmark on the detection performance of the proposed solutions. Nevertheless, at this stage the proposed approaches already provided *secure* solutions for the localization problem; thus, one can estimate δ_i and σ according to the ML criterion by exploiting $\hat{\boldsymbol{x}}$ as

$$\widehat{\delta}_i = \frac{\sum_{k=1}^{K}\hat{\theta}_{i,k}}{K},$$

and

$$\widehat{\sigma} = \frac{\sum_{i=1}^{N}\sqrt{\frac{\sum_{k=1}^{K}\left(\hat{\theta}_{i,k} - \widehat{\delta}_i\right)^2}{K-1}}}{N},$$

with $\hat{\theta}_{i,k} = P_0 - P_{i,k} - 10\gamma\log_{10}\frac{\|\hat{\boldsymbol{x}}-\boldsymbol{a}_i\|}{d_0}$.

Therefore, based on the minimum probability of error criterion [27, Ch. 3], one has that

$$\begin{aligned}P_E &= \text{Pr}\{\text{decide } \mathcal{H}_0|\mathcal{H}_1 \text{ true}\} + \text{Pr}\{\text{decide } \mathcal{H}_1|\mathcal{H}_0 \text{ true}\} \\ &= P(\mathcal{H}_0|\mathcal{H}_1)P(\mathcal{H}_1) + P(\mathcal{H}_1|\mathcal{H}_0)P(\mathcal{H}_0).\end{aligned} \tag{13}$$

Then, the following maximum (conditional) likelihood detector is derived from (13), which decides $\mathcal{H}_1$ if

$$\frac{p(\boldsymbol{\theta}|\mathcal{H}_1)}{p(\boldsymbol{\theta}|\mathcal{H}_0)} > \frac{P(\mathcal{H}_0)}{P(\mathcal{H}_1)}, \tag{14}$$

as shown in Appendix B. Note that (14) is similar to the Neyman–Pearson (NP) test, since the conditional likelihood ratio is compared to a threshold. However, in contrast to the NP test where one calculates the optimal threshold by maximizing P_D for a fixed probability of false alarm, P_{FA}, here, the threshold is determined by the quotient of the prior probabilities. Since the prior probabilities are equal in this case, we slightly modify the detection scheme by appropriately weighting the two errors in (13). This is accomplished by simply adjusting the threshold (which results into trading off miss and false alarm errors, but one cannot reduce them both simultaneously anyway) for our proposed detection scheme to decide $\mathcal{H}_1$ if

$$\frac{p(\boldsymbol{\theta}|\mathcal{H}_1)}{p(\boldsymbol{\theta}|\mathcal{H}_0)} > 3\widehat{\sigma}, \tag{15}$$

and decide $\mathcal{H}_0$ otherwise. Note that the choice of $3\widehat{\sigma}$ in (15) is clearly a sub-optimal one, and obviously other choices could be considered as well, but is sufficiently large to prevent having coin flipping (14) as the detection criterion.

IV. Performance Assessment

This section assesses the performance of the proposed estimators through computer simulations performed in MATLAB (version R2016b). The main interest is to analyze their performance against existing solutions, not only from the localization accuracy perspective, but also in terms of computational complexity and attacker detection rate.

A. Computational Complexity Analysis

In this section, a summary of the computational complexity together with the average running time (in seconds) of the proposed solutions and the state-of-the-art is provided. It is worth mentioning that the latter analysis was performed on

TABLE I: Computational Complexity and Average Running Time Analysis of the Considered Algorithms

Algorithm	Complexity	Average Duration (s)
R-SOCP in Section III-A	$\mathcal{O}\left(N^{3.5}\right)$	0.9
R-GTRS in Section III-B	$\mathcal{O}\left(T_{\max} \times N\right)$	0.014
SWLS in [19]	$\mathcal{O}\left(N\right)$	0.009
LC-GTRS in [20]	$\mathcal{O}\left(T_{\max} \times N\right)$	0.05

the machine with the following characteristics: CPU: INTEL CORE I7-4710HQ 2.5 GHZ, RAM: 16 GB, where $N = 6$, $\sigma = 3$ dB, and $\Delta = 8$ (dB), was considered in 10 Monte Carlo, M_c, runs. This analysis is pertinent, because it gives the reader a notion about the suitability of an algorithm to be implemented in real-time applications.

According to [28], the worst case computational complexity of an SOCP algorithm can be expressed by $\mathcal{O}\left(\sqrt{S}\left(c^2\sum_{r=1}^{S} s_r + \sum_{r=1}^{S} s_r^2 + c^3\right)\right)$, wits S denoting the number of the second-order cone (SOC) constraints, c is the number of the equality constraints, and s_r is the dimension of the r-th SOC in the derived SOCP problem. Moreover, given that $T_{\max}$ stands for the maximum number of bisection steps in the proposed R-GTRS approach and the existing LC-GTRS in [20], the worst-case computational complexity of the considered algorithms is presented in Table I. As expected, the result shows that the heaviest computational burden is suffered from the proposed R-SOCP estimator, while the remaining estimators have linear computational complexity in N. The results for time duration corroborate the ones of computational complexity showing that the three estimators with linear computational complexity are extremely fast, while the proposed R-SOCP requires somewhat more time to be executed, as anticipated.

B. Localization and Detection Performance

Here, the performance of the proposed solutions[3] is compared with the existing ones via computer simulations, from both localization accuracy and attacker detection perspectives. In the following simulations, all nodes were randomly placed $N_D = 1000$ times in a $25 \times 25\,\mathrm{m}^2$ area, and some of them (possibly all) might have been malicious/defective. The measurements were generated according to (1), with $P_0 = -10$ (dBm), $d_0 = 1$ (m), $\gamma = 3$, and $K = 10$, set as default, with the distance between any two nodes being at least 1 meter. For the SWLS estimator in [19], the threshold tuning parameter was set to $\zeta = 1.75$. For each node deployment, malicious reference points were chosen at random (ranging from none to all N reference points) $N_M = 100$ times. Possible attacks were executed independently by each malicious node, according to an exponential distribution[4], whose rate is drawn from a uniform distribution on the interval $[0, \Delta]$ (dB), i.e., $\delta_i \sim \pm\mathcal{E}(\mathcal{U}[0, \Delta])$, $\forall i$, if the i-th reference point is malicious, with $\pm$ denoting random sign attribution to δ_i. The principal metric used for assessing localization accuracy is the root mean squared error (RMSE), defined as $\text{RMSE} = \sqrt{\sum_{m=1}^{M_c} \frac{\|\boldsymbol{x}_m - \widehat{\boldsymbol{x}}_m\|^2}{M_c}}$, where $\widehat{\boldsymbol{x}}_m$ is the estimate of the true target location, $\boldsymbol{x}_m$, in the m-th M_c ($M_c = N_D \times N_M$) run. Lastly, it is worth mentioning that a lower bound on the localization performance of all algorithms (achieved through an exhaustive grid search (GS) of the ML function in (2)) is appended[5]. This brute force method is applied across the whole (25×25 (m^2)) region with 0.1 (m) increment in both x- and y- axes, and 1 (dB) increment for δ_i search.

Fig. 1 illustrates the RMSE (m) versus Δ (dB) performance comparison for different values of σ (dB) when $N = 5$. Naturally, the figure shows that the performance of all estimators deteriorates as σ grows. Clearly, the proposed approach shows superior performance over the existing ones, which is more evident for higher attack intensities for SWLS and for lower attack intensities for LC-GTRS. This result is not surprising, since the proposed approach (efficiently) takes advantage of the additional information[6] about Δ, from which the existing methods cannot benefit directly. It is also worth mentioning that, even though SWLS requires the true knowledge of σ, its performance is very much affected by the low number of reference points.

Fig. 2 illustrates the detection rate versus Δ (dB) performance comparison, for different values of σ (dB) when $N = 5$. The figure offers results for all considered algorithms in terms of "Correct" ($N_{CD}/(N_{CD}+N_{FD}+N_{ND})$), "False" ($N_{FD}/(N_{CD}+N_{FD}+N_{ND})$) and "No" ($N_{ND}/(N_{CD}+N_{FD}+N_{ND})$) attacker detection, with N_{CD}, N_{FD}, N_{ND} respectively denoting the no. of correctly detected attackers, the no. of incorrectly detected attackers, and the no. of non-detected attackers, together with the theoretical probability of detection, P_D, given in (11). At the first glance, the figure reveals modest detection performance of all estimators, which might be explained by elevated degree of the considered problem (the fact that multiple attackers might be present in the network and that the noise power is relatively high allowing attackers to disguise their malicious intents within the noise). As expected, Fig. 2 shows that LC-GTRS has the best detection performance, since this method relies on generalized likelihood ratio test (GLRT) to detect attackers in its complete three-step localization procedure, while the

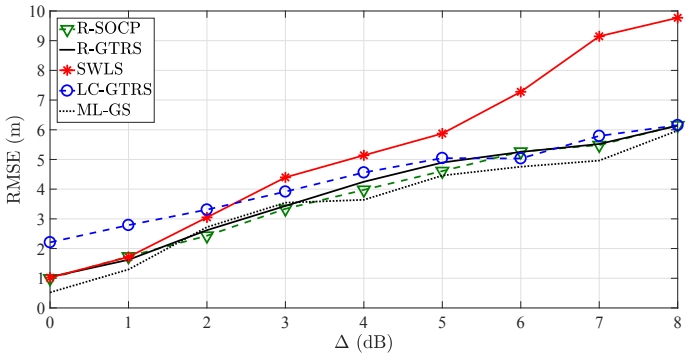
[3]Note that the results of the proposed R-SOCP estimator in (7) are shown in the following figures. Nevertheless, it is worth noting that, in all performed simulations, its performance was virtually identical to its strongly convex counterpart in (8) (considering $\epsilon = 10^{-32}$) and that its solution was always feasible.

[4]Notice that this setting guarantees that the assumed knowledge on the upper bound on the attack intensity, $|\delta_i| \leq \Delta$, is imperfect, which is clearly the case in practice. Nevertheless, it is worth mentioning that this choice of attack distribution is just one of many possibilities to achieve this guarantee.

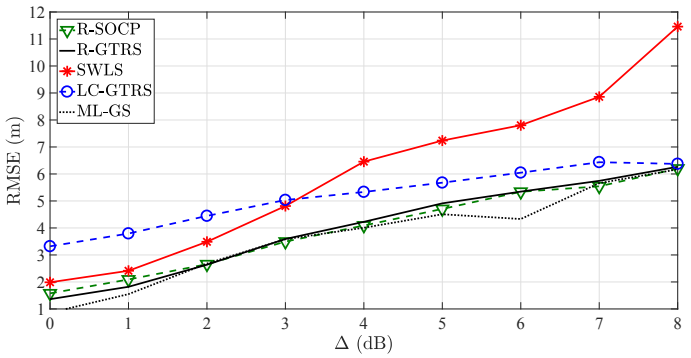
[5]Note that only $N_D = 10$ node deployments and $N_M = 5$ attacks were executed to obtain the presented results due to the extreme computational burden of the brute force method in the considered setting.

[6]A valid question that naturally arises is how to set an upper bound on the attack magnitude in practice, given that Δ is not perfectly available. Although not presented here, our simulations indicate that, as a rule of thumb, the assumed knowledge about Δ, $\tilde{\Delta}$, should be conservative (set $\tilde{\Delta}$ to a low value), since in that case the proposed approach suffers only mild degradation in its performance (for very low Δ), maintaining its performance for other values of Δ.

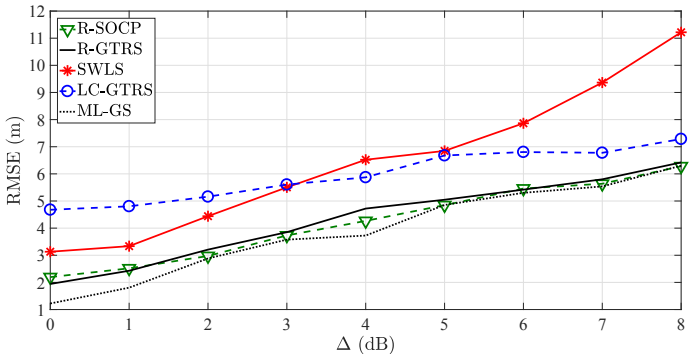
This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2023.3325063



(a) $\sigma = 1$ (dB)

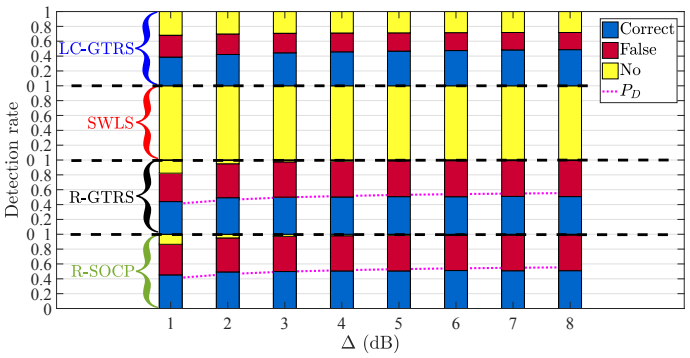


(b) $\sigma = 2$ (dB)

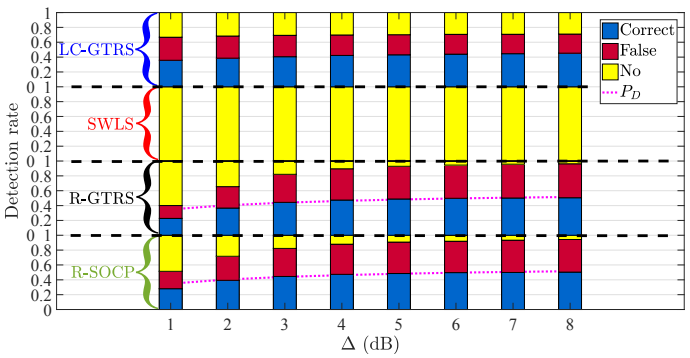


(c) $\sigma = 3$ (dB)

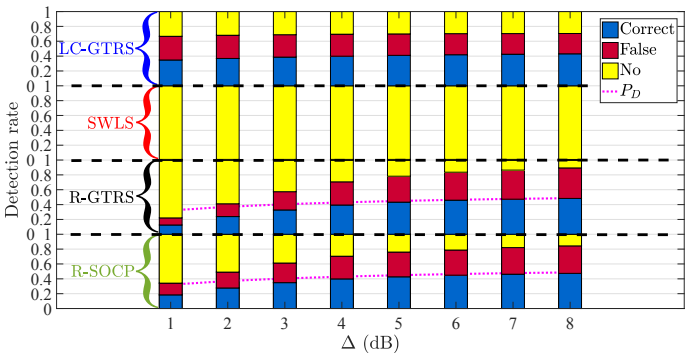
Fig. 1: RMSE (m) versus Δ (dB) illustration, for different choices of σ (dB), when $N = 5$.



(a) $\sigma = 1$ (dB)



(b) $\sigma = 2$ (dB)



(c) $\sigma = 3$ (dB)

Fig. 2: Detection rate versus Δ (dB) illustration, for different choices of σ (dB), when $N = 5$.

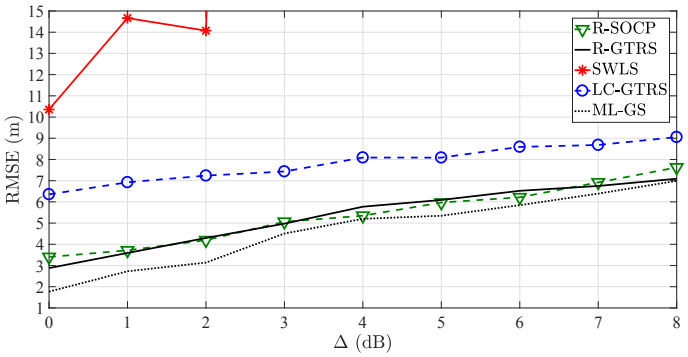
proposed schemes obtain their final localization solutions independently from detection, in a single step (where detection comes as a byproduct of an almost trivial approach). Moreover, one can see that the detection rate of the proposed methods corresponds closely to the theoretical results given by (12). Interestingly, it can be seen that for large attack intensities and $\sigma = 1$ (dB), the proposed detection schemes basically always detect attackers (either correctly or falsely), which could be adjusted by further spreading the threshold in (15). Finally, SWLS exhibits almost negligible detection performance. This is owed to the threshold tuning parameter, which had to be set fairly high ($\zeta = 1.75$) in order for SWLS to operate; otherwise, matrix singularity in the WLS procedure becomes an issues, retrieving very poor results.

Fig. 3 illustrates the RMSE (m) versus Δ (dB) performance comparison for different values of N when $\sigma = 3$ (dB). It can be seen that all estimators acquire significant performance boost with the increase of N. One can notice that SWLS practically does not work for the case of the bear minimum of reference points ($N = 4$) needed to solve the problem in 2-dimensional space. Once again, the proposed approach proves its worth, exhibiting the best overall performance.

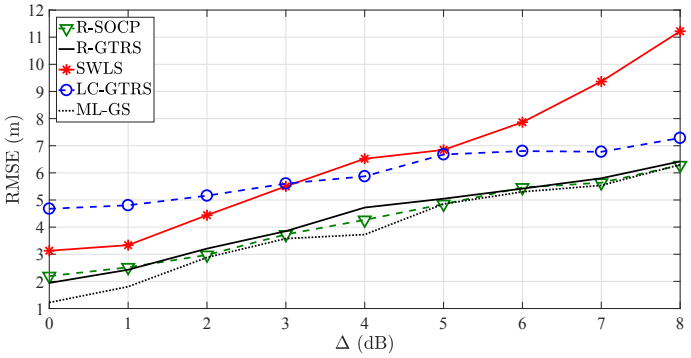
Fig. 4 illustrates the detection rate versus Δ (dB) performance comparison, for different values of N, when $\sigma = 3$ (dB). The figure exhibits considerable increase in the detection performance of the proposed approach with the growth of Δ. Once again, their detection performance tightly coincides with P_D and is very competitive with more a sophisticated GLRT scheme used in LC-GTRS method.

Fig. 5 illustrates the RMSE (m) versus different proportions

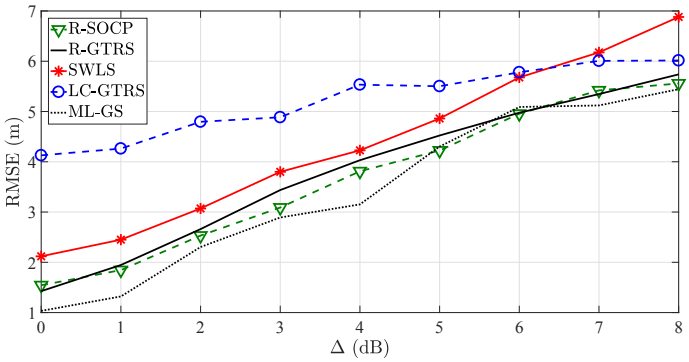
This article has been accepted for publication in IEEE Transactions on Vehicular Technology. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/TVT.2023.3325063



(a) $N = 4$

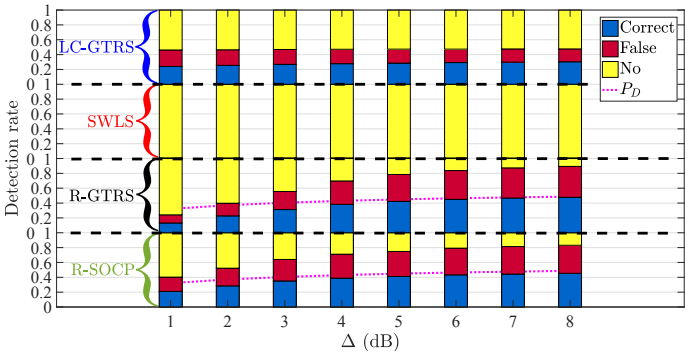


(b) $N = 5$

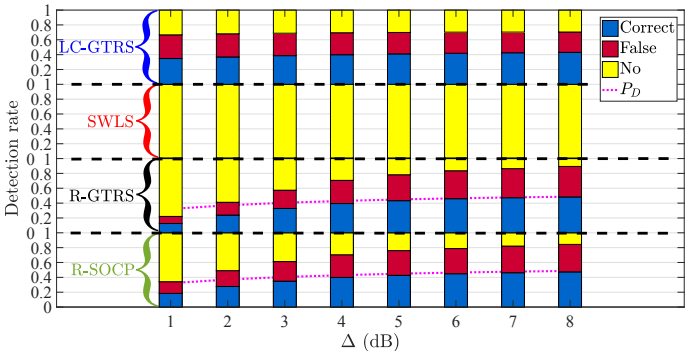


(c) $N = 6$

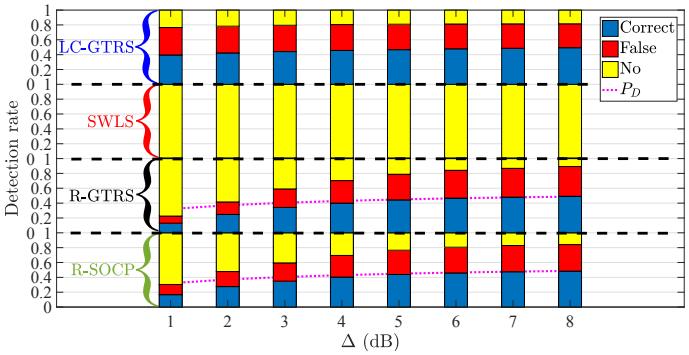
Fig. 3: RMSE (m) versus Δ (dB) illustration, for different choices of N, when $\sigma = 3$ (dB).



(a) $N = 4$



(b) $N = 5$



(c) $N = 6$

Fig. 4: Detection rate versus Δ (dB) illustration, for different choices of N, when $\sigma = 3$ (dB).

of the number of attackers, $\frac{N_A}{N}$, performance comparison, when $N = 5$, $\Delta = 8$ (dB), and $\sigma = 1$ (dB). Fig. 5 clearly corroborates the effectiveness of the proposed solutions, showing that they achieve practically constant localization accuracy for $\frac{N_A}{N} \geq 40\%$, whereas the performance of the existing methods deteriorates when the number of attackers present in the network grows in general.

To conclude the results analysis, Fig. 6 illustrates the cumulative distribution function (CDF) of the localization error (LE), defined as LE $= \|\boldsymbol{x}_m - \widehat{\boldsymbol{x}}_m\|$ (m) in the m-th M_c run, for $N = 6$, $\sigma = 3$ (dB) and $\Delta = 3$ (dB). The figure shows that LC-GTRS start off well and has the best median, but it finishes of poorly, while the proposed estimators start off somewhat more modestly, but outperform the existing ones overall, achieving LE ≤ 5 meters in above 90% of the cases,

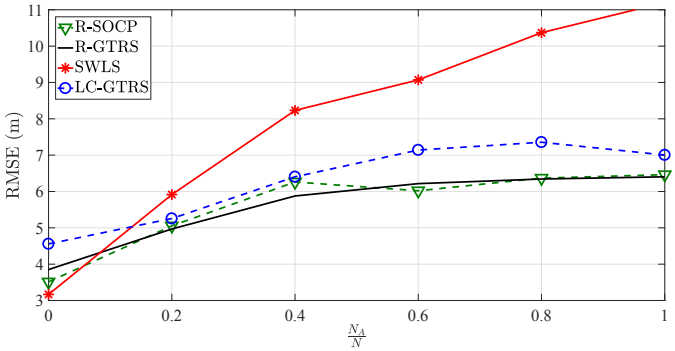


Fig. 5: RMSE (m) versus $\frac{N_A}{N}$ illustration, for $N = 5$, $\Delta = 8$ (dB), and $\sigma = 1$ (dB).

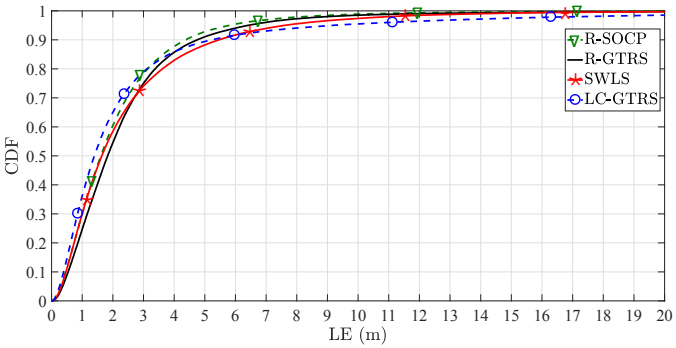


Fig. 6: CDF versus LE (m) illustration, for $N = 6$, $\sigma = 3$ (dB) and $\Delta = 3$ (dB).

whereas the other estimators achieve this aim in below 90% of the cases[7].

V. Conclusions

This work addressed an actual and nowadays a very pertinent topic of secure target localization in wireless networks in the presence of malicious attackers. It introduced a novel mim-max approach for secure localization in the presence of malicious attackers. Unlike the existing approaches, the proposed one treats all devices as malicious at the beginning and is based on the worst-case study of the problem, by assuming that (imperfect) knowledge about the upper-bound on the attack intensity is known. In this way, the proposed approach allowed us to mitigate the influence of the malicious attacks by treating them as nuisance parameters. This led to two possible directions that resulted in the derivation of two robust estimators: SOCP- and GTRS-based. The former one has somewhat higher computational burden, but showed a slightly better localization accuracy, while the latter one is computationally light and virtually matches the performance of the more complex one. The work proposed a modified maximum (conditional) likelihood detector for attacker detection and presented an analysis on achievable detection performance. In summary, the proposed approach works well regardless of the number of attackers present in the network and its biggest advantage over the existing solutions is that it can even cope with the case where all reference points are malicious. Its detection performance is closely in line with theory and is competitive (for large attack intensities) with more sophisticated approaches used in existing solutions.

Appendix A
The Proposed Robust Approach in a General Range-based Setting

Here, a general range-based model is considered as

$$d_{i,k} = \|\boldsymbol{x} - \boldsymbol{a}_i\| + \delta_i + n_{i,k}, \tag{16}$$

[7]Besides the presented results, it is worth mentioning that the effect of K was also studied in our simulations, considering values up to $K = 100$. The results are omitted here, but the main conclusions are consistent with the ones drawn in this section, with slight improvements in (both localization and detection) performance for bigger K for all methods, as expected.

where $n_{i,k} \sim \mathcal{N}(0, \sigma_{i,k}^2)$ represents the measurement error. Similarly as before, we use the median of all K measurements, d_i, and drop the subscript k.

Start by subtracting $\frac{\Delta}{4}$ from both sides of (16) to get

$$\lambda_i = \|\boldsymbol{x} - \boldsymbol{a}_i\| + \rho_i + n_i, \tag{17}$$

where $\lambda_i = d_i - \frac{\Delta}{4}$ and $\rho_i = \delta_i - \frac{\Delta}{4}$. Loosely speaking, by rearranging and squaring (17), followed by disregarding the second-order noise term, gives

$$n_i \approx \frac{(\lambda_i - \rho_i)^2 - \|\boldsymbol{x} - \boldsymbol{a}_i\|^2}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|}. \tag{18}$$

The following min-max problem is derived from (18)

$$\underset{\boldsymbol{x}}{\text{minimize}} \ \underset{\rho_i}{\text{maximize}} \sum_{i=1}^{N} \left(\frac{(\lambda_i - \rho_i)^2 - \|\boldsymbol{x} - \boldsymbol{a}_i\|^2}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|} \right)^2. \tag{19}$$

By defining $f(\rho_i) = \frac{\left|(\lambda_i - \rho_i)^2 - \|\boldsymbol{x} - \boldsymbol{a}_i\|^2\right|}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|}$, the problem in (19) becomes equivalent to

$$\underset{\boldsymbol{x}}{\text{minimize}} \ \underset{\rho_i}{\text{maximize}} \sum_{i=1}^{N} f(\rho_i)^2.$$

Moreover, since

$$\underset{\rho_i}{\text{maximize}} \sum_{i=1}^{N} f(\rho_i)^2 = \sum_{i=1}^{N} \left[\underset{\rho_i}{\text{maximize}} \, f(\rho_i) \right]^2,$$

and, by definition

$$|\rho_i| = \left| \delta_i - \frac{\Delta}{4} \right| \leq \frac{3\Delta}{4},$$

it follows that

$$\underset{\rho_i}{\text{maximize}} f(\rho_i) = \begin{cases} f\left(-\frac{3\Delta}{4}\right), & \text{if } f\left(-\frac{3\Delta}{4}\right) \geq f\left(\frac{3\Delta}{4}\right) \\ f\left(\frac{3\Delta}{4}\right), & \text{if } f\left(-\frac{3\Delta}{4}\right) < f\left(-\frac{3\Delta}{4}\right) \end{cases},$$

with

$$f\left(-\frac{3\Delta}{4}\right) = \frac{\left|\left(\lambda_i + \frac{3\Delta}{4}\right)^2 - \|\boldsymbol{x} - \boldsymbol{a}_i\|^2\right|}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|}$$

and

$$f\left(\frac{3\Delta}{4}\right) = \frac{\left|\left(\lambda_i - \frac{3\Delta}{4}\right)^2 - \|\boldsymbol{x} - \boldsymbol{a}_i\|^2\right|}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|}.$$

One bypasses tackling (19) directly by minimizing its upper bound, i.e.,

$$\begin{aligned} \underset{\boldsymbol{x}}{\text{minimize}} & \sum_{i=1}^{N} \left(\frac{\left(d_i + \frac{\Delta}{2}\right)^2 - \|\boldsymbol{x} - \boldsymbol{a}_i\|^2}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|} \right)^2 \\ & + \sum_{i=1}^{N} \left(\frac{(d_i - \Delta)^2 - \|\boldsymbol{x} - \boldsymbol{a}_i\|^2}{2\|\boldsymbol{x} - \boldsymbol{a}_i\|} \right)^2. \end{aligned} \tag{20}$$

A. R-SOCP estimator

By following a similar approach as in Section III-A, (20) is relaxed into the following SOCP problem.

$$\underset{\boldsymbol{x},y,\boldsymbol{e},\boldsymbol{t}}{\text{minimize}}\ \mathbf{1}_{1\times N}\boldsymbol{e}+\mathbf{1}_{1\times N}\boldsymbol{t} \tag{21a}$$

subject to

$$\left\|\begin{bmatrix}2\boldsymbol{x}\\ y-1\end{bmatrix}\right\|\leq y+1, \tag{21b}$$

$$\begin{aligned}&\left\|\begin{bmatrix}2\left(\left(d_i+\frac{\Delta}{2}\right)^2-y+2\boldsymbol{a}_i^T\boldsymbol{x}-\|\boldsymbol{a}_i\|^2\right)\\ 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-e_i\end{bmatrix}\right\|\\ &\leq 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)+e_i,\ \ i=1,...,N,\end{aligned} \tag{21c}$$

$$\begin{aligned}&\left\|\begin{bmatrix}2\left((d_i-\Delta)^2-y+2\boldsymbol{a}_i^T\boldsymbol{x}-\|\boldsymbol{a}_i\|^2\right)\\ 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)-t_i\end{bmatrix}\right\|\\ &\leq 4\left(y-2\boldsymbol{a}_i^T\boldsymbol{x}+\|\boldsymbol{a}_i\|^2\right)+t_i,\ \ i=1,...,N,\end{aligned}. \tag{21d}$$

B. R-GTRS estimator

By introducing weights, $w_i=\frac{d_i^{-1}}{\sum_{i=1}^N d_i^{-1}}$, and following a similar approach as in Section III-B one gets

$$\begin{aligned}\underset{\boldsymbol{x}}{\text{minimize}}&\sum_{i=1}^N w_i\left(\frac{\left(d_i+\frac{\Delta}{2}\right)^2-\|\boldsymbol{x}-\boldsymbol{a}_i\|^2}{2d_i}\right)^2\\ &+\sum_{i=1}^N w_i\left(\frac{(d_i-\Delta)^2-\|\boldsymbol{x}-\boldsymbol{a}_i\|^2}{2d_i}\right)^2,\end{aligned}$$

which can be written in the GTRS form as

$$\underset{\boldsymbol{y}=[\boldsymbol{x},\,\|\boldsymbol{x}\|^2]^T}{\text{minimize}}\left\{\|\boldsymbol{H}\boldsymbol{y}-\boldsymbol{h}\|^2:\ \ \boldsymbol{y}^T\boldsymbol{B}\boldsymbol{y}+2\boldsymbol{b}^T\boldsymbol{y}=0\right\}, \tag{22}$$

where $\boldsymbol{H}\in\mathbb{R}^{2N\times 3}$ and $\boldsymbol{h}\in\mathbb{R}^{2N}$ are given by

$$\boldsymbol{H}=\boldsymbol{W}\begin{bmatrix}\vdots & \vdots\\ 2\boldsymbol{a}_i^T & -1\\ \vdots & \vdots\\ 2\boldsymbol{a}_i^T & -1\\ \vdots & \vdots\end{bmatrix},\ \ \boldsymbol{h}=\boldsymbol{W}\begin{bmatrix}\vdots\\ \|\boldsymbol{a}_i\|^2-(d_i+\frac{\Delta}{2})^2\\ \vdots\\ \|\boldsymbol{a}_i\|^2-(d_i\Delta)^2\\ \vdots\end{bmatrix},$$

$$\boldsymbol{B}=\begin{bmatrix}\boldsymbol{I}_2 & \mathbf{0}_{2\times 1}\\ \mathbf{0}_{1\times 2} & 0\end{bmatrix}\in\mathbb{R}^{3\times 3},\ \boldsymbol{b}=\begin{bmatrix}\mathbf{0}_{2\times 1}\\ -0.5\end{bmatrix}\in\mathbb{R}^3,$$

with $\boldsymbol{W}=\text{diag}\left(\left[...,\sqrt{w_i},...,\sqrt{w_i},...\right]^T\right)\in\mathbb{R}^{2N\times 2N}$.

APPENDIX B
DERIVATION OF THE MAXIMUM LIKELIHOOD DETECTOR

By letting $R_1=\{\boldsymbol{\theta}:\text{decide }\mathcal{H}_1\}$ denote the critical region and R_0 to be its complement [27, Ch. 3], from (13), one has that

$$\begin{aligned}P_E&=P(\mathcal{H}_1)\int_{R_0}p(\boldsymbol{\theta}|\mathcal{H}_0)d\boldsymbol{\theta}+P(\mathcal{H}_0)\int_{R_1}p(\boldsymbol{\theta}|\mathcal{H}_1)d\boldsymbol{\theta}\\ &=P(\mathcal{H}_1)+\int_{R_1}P(\mathcal{H}_0)p(\boldsymbol{\theta}|\mathcal{H}_0)-P(\mathcal{H}_1)p(\boldsymbol{\theta}|\mathcal{H}_1)d\boldsymbol{\theta},\end{aligned}$$

by using the identity $\int_{R_0}p(\boldsymbol{\theta}|\mathcal{H}_0)d\boldsymbol{\theta}=1-\int_{R_1}p(\boldsymbol{\theta}|\mathcal{H}_0)d\boldsymbol{\theta}$.

It follows that $\boldsymbol{\theta}\in R_1$ if the integrand in the above expression is negative, i.e., one decides $\mathcal{H}_1$ if

$$P(\mathcal{H}_0)p(\boldsymbol{\theta}|\mathcal{H}_0)<P(\mathcal{H}_1)p(\boldsymbol{\theta}|\mathcal{H}_1),$$

which is equivalent to deciding $\mathcal{H}_1$ if

$$\frac{p(\boldsymbol{\theta}|\mathcal{H}_1)}{p(\boldsymbol{\theta}|\mathcal{H}_0)}>\frac{P(\mathcal{H}_0)}{P(\mathcal{H}_1)}.$$

ACKNOWLEDGEMENT

The authors would like to express their sincere gratitude to Prof. João Xavier from the Institute of Systems and Robotics, Instituto Superior Técnico, Lisbon, Portugal for his generous contribution in addressing the feasibility and continuity issues of the proposed R-SOCP solution. The authors would also like to thank the associate editor, Prof. Kaigui Bian, and the anonymous reviewers for their valuable comments and suggestions which improved the quality of the paper.

REFERENCES

[1] Q. L. Tian, K. I. K. Wang, and Z. Salcic, "RA Low-Cost INS and UWB Fusion Pedestrian Tracking System," *IEEE Sensors Journal*, vol. 19, no. 10, pp. 3733–3740, May 2019.

[2] J. P. Matos-Carvalho, R. Santos, S. Tomic, and M. Beko, "GTRS-based Algorithm for UAV Navigation in Indoor Environments Employing Range Measurements and Odometry," *IEEE Access*, vol. 9, pp. 89120–89132, June 2021.

[3] A. Coluccia and A. Fascista, "On the Hybrid TOA/RSS Range Estimation in Wireless Sensor Networks," *IEEE Transactions on Wireless Communications,* vol. 17, no. 1, pp. 361–371, January 2018.

[4] S. Tomic, M. Beko and R. Dinis, "3-D Target Localization in Wireless Sensor Network Using RSS and AoA Measurement," *IEEE Transactions on Vehicular Technology,* vol. 66, no. 4, pp. 3197–3210, April 2017.

[5] A. Fascista, A. Coluccia, H. Wymeersch, and G. Seco-Granados, "Millimeter-Wave Downlink Positioning With a Single-Antenna Receiver," *IEEE Transactions on Wireless Communications,* vol. 18, no. 9, pp. 4479–4490, September 2019.

[6] S. Tomic and M. Beko, "A Geometric Approach for Distributed Multihop Target Localization in Cooperative Networks," *IEEE Transactions on Vehicular Technology,* vol. 69, no. 1, pp. 914–919, January 2020.

[7] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends," *Proceedings of the IEEE*, vol. 104, no. 9, pp. 1727–1765, September 2016.

[8] S. Capkun and J. P. Hubaux, "Secure Positioning in Wireless Networks," *IEEE Journal on Selected Areas in Communications,* vol. 24, no. 2, pp. 221–232, February 2006.

[9] M. Singh, P. Leu, A. R. Abdou, and S. Capkun, "UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband," *USENIX Security Simposium,* Santa Clara, CA, USA, pp. 73–88, August 2019.

[10] D. Liu, N. Ning, A. Liu, C. Wang, and W. K. Du, "Attack-resistant Location Estimation in Wireless Sensor Networks," *ACM Transactions on Information and System Security,* vol. 11, no. 4, pp. 1–39, July 2008.

[11] D. He, L. Cui, H. Huang, and M. Ma, "Design and Verification of Enhanced Secure Localization Scheme in Wireless Sensor Networks," *IEEE Transactions on Parallel and Distributed Systems,* vol. 20, no. 7, pp. 1050–1058, July 2009.

[12] R. Garg, A. L. Varna, and M. Wu, "An Efficient Gradient Descent Approach to Secure Localization in Resource Constrained Wireless Sensor Networks," *IEEE Transactions on Information Forensics and Security,* vol. 7, no. 2, pp. 717–730, April 2012.

[13] X. Liu, S. Su, F. Han, Y. Liu, and Z. Pan, "A Range-Based Secure Localization Algorithm for Wireless Sensor Networks," *IEEE Sensors Journal,* vol. 19, no. 2, pp. 785–796, January 2019.

[14] J. Won and E. Bertino, "Robust Sensor Localization against Known Sensor Position Attacks," *IEEE Transactions on Mobile Computing,* vol. 18, no. 2, pp. 2954–2967, December 2019.

[15] X. Huan, K. S. Kim, and J. Zhang, "NISA: Node Identification and Spoofing Attack Detection Based on Clock Features and Radio Information for Wireless Sensor Networks," *IEEE Transactions on Communications,* vol. 69, no. 7, pp. 4691–4703, July 2021.

[16] B. Mukhopadhyay, S. Srirangarajan, and K. Kar, "Robust Range-based Secure Localization in Wireless Sensor Networks," *IEEE GLOBECOM,* Abu Dhabi, UAE, pp. 1–6, December 2018.

[17] Y. Li, S. Ma, G. Yang, and K. K. Wong, "Secure Localization and Velocity Estimation in Mobile IoT Networks With Malicious Attacks," *IEEE Internet of Things Journal,* vol. 8, no. 8, pp. 6878–6892, April 2021.

[18] M. Beko and S. Tomic, "Towards Secure Localization in Randomly Deployed Wireless Networks," *IEEE Internet of Things Journal,* vol. 8, no. 24, pp. 17436–17448, December 2021.

[19] B. Mukhopadhyay, S. Srirangarajan, and S. Kar, "RSS-Based Localization in the Presence of Malicious Nodes in Sensor Networks," *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 5503716–5503716, August 2021.

[20] S. Tomic and M. Beko, "Detecting Distance-spoofing Attacks in Arbitrarily-deployed Wireless Networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 4, pp. 4383–4395, April 2022.

[21] M. Grant and S. Boyd, "CVX: Matlab Software for Disciplined Convex Programming," ver. 1.21. http://cvxr.com/cvx, May 2010 [Online]. Available: http://cvxr.com/cvx

[22] A. Beck, P. Stoica, and J. Li, "Exact and Approximate Solutions of Source Localization Problems," *IEEE Transactions on Signal Processing* vol. 56, no. 5, pp. 1770–1778, May 2008.

[23] T. Rappaport, *Wireless Communications: Principles and Practice*. Prentice-Hall, Upper Saddle River, NJ, USA: Prentice-Hall, 1996.

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

[25] S. Boyd and L. Vanderberghe, *Convex Optimization*. Cambridge University Press, Cambridge, UK, 2004.

[26] S. Tomic, M. Beko, R. Dinis, M. Tuba, and N. Bacanin. *RSS-AoA-based Target Localization and Tracking in Wireless Sensor Networks.* River Publishers Series in Communications, River Publishers, Alsbjergvej 10, Gistrup, Denmark, 2017.

[27] S. M. Kay. *Fundamentals of Statistical Signal Processing: Detection Theory.* Prentice-Hall: Upper Saddle River, NJ, USA, 1998.

[28] I. Polik, T. Terlaky, "Interior Point Methods for Nonlinear Optimization," *Nonlinear Optimization*, 1st ed.; Di Pillo, G., Schoen, F., Eds.; Springer: Heidelberg/Berlin, Germany, 2010; Volume 1989, pp. 215–276.

Slavisa Tomic received the M.S. degree in traffic engineering according to the postal traffic and telecommunications study program from University of Novi Sad, Serbia, in 2010, and the PhD degree in electrical and computer engineering from University Nova of Lisbon, Portugal, in 2017. He is currently an Assistant Professor at the Universidade Lusófona de Humanidades e Tecnologias, Lisbon, Portugal. He is one of the winners of the 4th edition of Scientific Employment Stimulus (CEEC Individual 2021) funded by Fundação para a Ciência e a Tecnologia. According to the methodology proposed by Stanford University, he was among the most influential researchers in the world between 2019 and 2022 when he joined the list of top 2% of scientists whose work is most cited by other colleagues in the field of Information and Communication Technologies, sub-area Networks and Telecommunications. His research interests include target localization in wireless sensor networks, and non-linear and convex optimization.

Marko Beko was born in Belgrade, Serbia, in November 1977. He received the Ph.D. degree in electrical and computer engineering from the Instituto Superior Técnico (IST), Universidade de Lisboa, Portugal, in 2008. He received the title of a "Professor with Habilitation" of electrical and computer engineering from the Universidade Nova de Lisboa, Lisbon, in 2018. His current research interests lie in the area of signal processing for wireless communications. He serves as an Associate Editor for the IEEE Open Journal of the Communications Society. He is also a member of the Editorial Board of IEEE Open Journal of Vehicular Technology. He is the winner of the 2008 IBM Portugal Scientific Award. According to the methodology proposed by Stanford University, he was among the most influential researchers in the world between 2019 and 2022 when he joined the list of top 2% of scientists whose work is most cited by other colleagues in the field of Information and Communication Technologies, sub-area Networks and Telecommunications. He is one of the founders of Koala Tech.