Trustworthy Target Localization via ADMM in the Presence of Malicious Nodes

Slavisa Tomic and Marko Beko

***Abstract*—Similar to numerous problems that gain interest nowadays (like the ones arising in statistics and machine learning), target localization problem can be cast in the framework of convex optimization. Nevertheless, owing to recent eruption in both size and heterogeneity of modern wireless networks which exposes them to various security threats, it is increasingly important to be able to localize the target reliably (securely). On the one hand, the security feature precludes the direct use of most existing localization algorithms in modern networks, since these are vulnerable to malicious attacks (for instance, measurement spoofing). On the other hand, taking security menace into consideration often leads to an under-determined problem formulation which requires certain approximations/relaxations of the problem, resulting in insufficiently accurate solutions. This work argues that the alternating direction method of multipliers (ADMM) is a well tailored approach to combat the secure localization problem. The proposed solution is a decomposition-coordination scheme, where solutions to smaller local (sub-) problems are bound together to obtain a solution to a larger global problem. To this end, an equivalent reformulation of the (non-convex) maximum likelihood estimator (MLE) as a smooth constrained non-convex minimization problem is derived first, which gives rise to a simple iterative scheme that does not require further approximations nor convex relaxations. The performance of the proposed algorithm is corroborated through computer simulations and experimental measurements.**

***Index Terms*—Alternating direction method of multipliers (ADMM), measurement-spoofing, probability of detection, reliable localization, generalized likelihood ratio test (GLRT), secure localization.**

I. Introduction

TO ACCOMMODATE the escalating requirements of next generation wireless applications, like self-driving ground and air vehicles [1], industrial and tactile internet-of-things (IoT) [2], [3], digital twins [4] and Internet of Underwater Things [5] to name a few, the research, innovation and industrial communities are relying on millimeter wave communications [6], terahertz [7], and optical bands [8]. Even though these systems offer extraordinary bandwidths, the aspired quality of service in terms of throughput, latency, and reliability in acceptable transmission distances can only be achieved if the end devices know each other's relative location [9]. Consequently, localization will play a crucial role in such wireless systems [10]. Nonetheless, if the location information is not reliable or is manipulated (spoofed), it can lead to disastrous consequences. Therefore, achieving trustworthy localization will be of paramount importance for high frequency systems.

During the last few years, secure localization problem captured a lot of attention in the scientific community [11]–[22]. According to the existing literature, one can distinguish between uncoordinated (each malicious attacker acts independently from others) and coordinated (a group of malicious attackers collaborates together) spoofing attacks. The recent work in [18], proposed a weighted least squares (WLS) estimator for received signal strength (RSS)-based localization, under uncoordinated attacks. This estimator was designed by considering a proper weight definition suitable for log-distance model, where smaller weights are assigned to *remote* devices and vice versa. In [19], a clustering method based on circle intersections after which a threshold-based keying scheme is applied to identify attackers, which are then eliminated from a non-linear localization process transformed into a generalized trust region sub-problem (GTRS) framework was described. However, the work in [19] considered only distance-enlargement attacks, by studying the employment of two-way time of arrival (TOA) measurements. The authors of both [18] and [19] updated their works recently by introducing a new secure WLS (SWLS) and l_1-norm-based techniques (termed LN-1 and LN-1E) together with a 3-D plane fitting solved by standard alternating direction method of multipliers (ADMM) method for RSS-based localization [20], and by considering a common range-based measurement model where law of cosines (LC) was applied to cast the problem into a GTRS framework [21], respectively. In [22], the authors developed a robust secure localization approach by studying the worst-case scenario in which all devices are assumed malicious from the beginning. The malicious attacks were treated as nuisance parameters in order to apply a min-max approach and formulate the secure localization problem as a robust non-linear least squares estimator. This estimator is then relaxed into a second-order cone programming (R-SOCP) problem and robust GTRS (R-GTRS). Nonetheless, it is important to point out that, besides relying on

Manuscript received 23 February 2023; revised 8 October 2023; accepted 20 December 2023. Date of publication 10 January 2024; date of current version 16 May 2024. This work was supported in part by the European Union's Horizon Europe Research and Innovation Programme under the Marie Skłodowska-Curie Grant 101086387, in part by Fundação para a Ciência e a Tecnologia under Projects UIDB/04111/2020, UIDB/50008/2020, and in part by ROBUST under Grant EXPL/EEI-EEE/0776/2021 and 2021.04180.CEECIND. The review of this article was coordinated by Prof. Hongzi Zhu. *(Corresponding author: Slavisa Tomic.)*

Slavisa Tomic is with the COPELABS, Universidade Lusófona, 1749-024 Lisboa, Portugal (e-mail: slavisa.tomic@ulusofona.pt).

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

Digital Object Identifier 10.1109/TVT.2023.3346476

the a priori knowledge of the noise power and empirical tuning of a hyperparameter necessary to set a threshold for attacker detection, the generalization of the SWLS method [20] to a general range-based approach is not straightforward, since it is based on a non-linear relationship between RSS and distance. Furthermore, in order for the LC-GTRS approach in [21] to operate, the difference between genuine and corrupted devices needs to be at least $s+1$ (in an s-dimensional space). Lastly, the robust schemes in [22] necessitate knowledge on the upper bound of the attack intensity beforehand. Besides, the R-SOCP solution comes with a high computational burden which is not translated into any significant gain in comparison with R-GTRS.

In contrast to the state-of-the-art methods [18]–[22] that require additional knowledge and/or convex relaxations/approximations, this work proposes employing ADMM tool to elegantly address the secure localization problem. The new scheme is a decomposition-coordination approach, where solutions to smaller local (sub-) problems are integrated together to acquire a solution to a larger global problem. The proposed scheme starts with an analogous reformulation of the (non-convex) maximum likelihood (ML) estimator as a smooth constrained non-convex minimization problem, after which the benefits of dual decomposition and augmented Lagrangian methods for constrained optimization are blended together. The biggest advantage of the proposed method is that it does not require any further approximations nor convex relaxations, since the solutions to its smaller optimization problems are given by simple analytic formulas.

The main contributions of the present work are 3-fold, and are summarized as follows:

- The current work presents a novel solution for trustworthy target localization in arbitrarily-deployed wireless networks in the presence of malicious (or defective) nodes that are able to manipulate (spoof) their distance measurements. The proposed solution outperforms the existing ones in both cases of uncoordinated and coordinated attacks, and does not require any prior knowledge regarding the type of the attacks.
- Unlike most of existing solutions that are derived based on squared range least squares approach, where the least squared error is minimized in the squared domain and has no statistical interpretation, the proposed approach is based on (weighted) least squares, where the squared (weighted) sum of errors is minimized and can be interpreted as an ML estimator whenever the noise is assumed Gaussian. Moreover, in contrast to the existing approaches, the proposed scheme requires no additional relaxations/approximations, since it benefits from dual decomposition and augmented Lagrangian methods for constrained optimization.
- The proposed work applies a series of mathematical manipulations on the considered system model to transform it into a suitable form, where by variable splitting (to obtain an equivalent, but constrained optimization problem) and augmented Lagrangian framework (to deal with the derived optimization problem) the problem is elegantly solved via ADMM algorithm.

The remainder of this work is organized as follows. Section II introduces a general model for (compromised) range measurements and provides a mathematical definition of the considered problem. In Section III, a detailed derivation of the proposed solution based on ADMM is presented, together with a detection scheme to identify an anchor as genuine or malicious. Section IV validates the performance of the proposed solution both in terms of complexity (computational and temporal) and accuracy (localization and attacker detection), while Section V concludes the work.

II. Problem Formulation

Let $\boldsymbol{a}_i \in \mathbb{R}^s$, $i=1,\ldots,N$, denote the true locations of N stationary reference nodes (anchors) and $\boldsymbol{x} \in \mathbb{R}^s$ the true location of a target, with $s=2$ or 3. The true locations of the anchors are known a priori, whereas determining the location of the target is the main goal of this work. The assumption that the target and anchors can communicate with each other and that the anchors possess suitable equipment so that they can retrieve range measurements from the received radio signal (e.g., through TOA or RSS observations) is taken for granted. Moreover, a subset of anchors ($\leq 50\%$ of the total) are assumed malicious or impaired, so that their measurements tend to obstruct the localization endeavor. The adverse attacks can be achieved by manipulating (spoofing) range measurements (for instance, by changing the transmit power levels) or can simply occur due to hardware impairments. Generally, the literature on secure localization problem [13], [19], [20], distinguishes between uncoordinated (compromised anchors act individually and independently from one another) and coordinated attacks (a group of compromised anchors collaborates together). It is important to note that, in practice, one cannot possibly know under what type of attacks the network is beforehand. Nevertheless, in any case, the adverse deeds are considered here as non-cryptographic, meaning that the perpetrators take no risk of impinging upper-layer security protocols when performing strikes.

Mathematically, in its general form, secure range-based localization problem can be formulated as a system of non-linear equations, where the equations describe the observed ranges between the anchors and the target as being their respective distances contaminated with additive noise and possibly a malicious attack [21]. Therefore, the k-th distance measurement sample ($1 \leq k \leq K$) between the target and the i-th anchor (in meters) can be modeled [23]–[25] as

$$d_{i,k} = \|\boldsymbol{x} - \boldsymbol{a}_i\| + \delta_i + n_{i,k}, \tag{1}$$

where $n_{i,k}$ denotes 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. Note that the case where $\delta_i = 0$ corresponds to anchor i not being compromised, while the case where $\delta_i \neq 0$ corresponds to anchor i being compromised.

The system model presented in (1) corresponds to the one used in [26], where the authors used a satellite simulator to demonstrate that it is possible to take over the victim's satellite lock and spoof its GPS receiver. This was done by manually

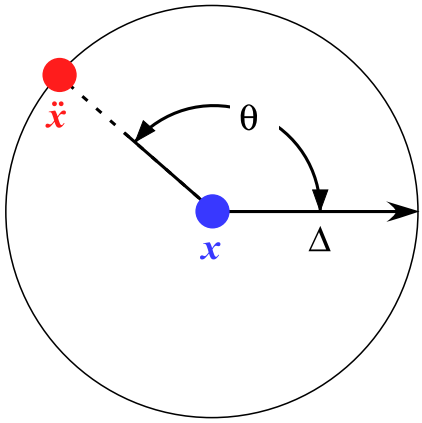

Fig. 1. Illustration of the determination process of $\ddot{\boldsymbol{x}}$: θ (rad) and Δ (m) respectively denote arbitrarily chosen angle and radius around $\boldsymbol{x}$.

placing an antenna close to the victim's receiver (mounted in a truck) to lock it, after which the spoofing signal could actually be transmitted from a greater distance. It also corresponds to the model presented in [27], where the authors illustrated an example for distance reduction attacks as hijacking a car in a street by using a relay system to trick the car into thinking that the key is in its vicinity, when it actually is not.

Some works (e.g., [13], [20]) model coordinated attacks according to

$$d_{i,k} = \begin{cases} \|\ddot{\boldsymbol{x}} - \boldsymbol{a}_i\| + n_{i,k}, & \text{if } i \text{ is compromised} \\ \|\boldsymbol{x} - \boldsymbol{a}_i\| + n_{i,k}, & \text{otherwise} \end{cases},$$

where $\ddot{\boldsymbol{x}}$ denotes an arbitrary point agreed by the collaborating attackers; we kindly refer the reader to see Fig. 1. Nevertheless, the above model is just a special case of (1), when $\delta_i = \|\ddot{\boldsymbol{x}} - \boldsymbol{a}_i\| - \|\boldsymbol{x} - \boldsymbol{a}_i\|$, and for this reason the current work considers (1) as the general model for both uncoordinated and coordinated spoofing attacks.

Lastly, for the sake of simplicity and without loss of generality, in the text that follows, the median of the K distance observations, d_i, is computed and used as observation of anchor i, while the measurement variances are taken as identical for any link i (and sample k), i.e., $\sigma_1^2 = \sigma_2^2 = \ldots = \sigma_N^2 = \sigma^2$.

By taking advantage of the distance observations in (1) and according to the ML principle [28, Ch. 7], the target can be localized by minimizing the squared sum of noise errors as

$$\widehat{\boldsymbol{x}} = \arg\min_{\boldsymbol{x},\delta_i} \sum_{i=1}^{N} \frac{1}{\sigma^2} \left(\|\boldsymbol{x} - \boldsymbol{a}_i\| + \delta_i - d_i\right)^2. \tag{2}$$

Even though the ML approach is a frequently employed approach in practice generally, the estimator in (2) is underdetermined, non-convex and non-smooth. Unlike most of the existing approaches that avoid direct tackling of (2) by applying certain relaxation/approximation techniques, the current work does not seek any circumvention of the problem. Instead, a new simple and iterative approach is introduced to tackle (2) directly by casting it as an equivalent smooth constrained non-convex minimization problem. The non-convexity of the derived estimator is dealt with locally, by binding together solutions of individual sub-problems to get a solution of the global problem.

III. The Proposed Approach for the Secure Localization Problem

This section describes a detailed derivation of the proposed ADMM-based solution for the localization problem, and provides an overview of the employed attacker detection scheme. Thus, it is organized correspondingly.

A. ADMM-Based Target Localization

First, weights $w_i = \frac{d_i^{-1}}{\sum_{i=1}^{N} d_i^{-1}}$ are brought into play in order to attribute more confidence to closer links. Then, by developing the square in (2) and dropping the constant terms (which have no impact on the minimization), one gets

$$\min_{\boldsymbol{x},\delta_i} \sum_{i=1}^{N} w_i \left(\|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - 2(d_i - \delta_i)\|\boldsymbol{x} - \boldsymbol{a}_i\| - 2d_i\delta_i + \delta_i^2\right). \tag{3}$$

The problem in (3) is equivalent to

$$\underset{\boldsymbol{x},\delta_i,\boldsymbol{u}_i}{\text{minimize}} \left\{ \sum_{i=1}^{N} w_i \left(\frac{1}{2}\|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - d_i\boldsymbol{u}_i^T(\boldsymbol{x} - \boldsymbol{a}_i) + \delta_i\boldsymbol{u}_i^T(\boldsymbol{x} - \boldsymbol{a}_i) - d_i\delta_i + \frac{1}{2}\delta_i^2 \right) : \|\boldsymbol{u}_i\| = 1 \right\}, \tag{4}$$

where $\boldsymbol{u}_i$ is just a unit vector. This step aids to smooth out the objective function. Applying a sort of variable splitting to (4) and convexifying the constraint $\|\boldsymbol{u}_i\| = 1$ yields

$$\underset{\boldsymbol{x},\delta_i,\boldsymbol{u}_i,\boldsymbol{v}_i,\boldsymbol{h}_i,q_i}{\text{minimize}} \left\{ \sum_{i=1}^{N} w_i \left(\frac{1}{2}\|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \boldsymbol{v}_i^T(\boldsymbol{x} - \boldsymbol{a}_i) + \boldsymbol{h}_i^T(\boldsymbol{x} - \boldsymbol{a}_i) - q_i + \frac{1}{2}\delta_i^2 \right) : \|\boldsymbol{u}_i\| \le 1, \; d_i\boldsymbol{u}_i = \boldsymbol{v}_i, \delta_i\boldsymbol{u}_i = \boldsymbol{h}_i, d_i\delta_i = q_i \right\}. \tag{5}$$

The motivation for variable splitting is that sometimes it may be easier to solve the constrained version of a problem than it is to solve its unconstrained counterpart [29]. The augmented Lagrangian for the problem in (5) is then given by

$$L_\rho(\boldsymbol{x}, \boldsymbol{\delta}, \boldsymbol{u}, \boldsymbol{v}, \boldsymbol{h}, \boldsymbol{q}; \boldsymbol{\lambda}, \boldsymbol{\mu}, \boldsymbol{\nu}) = \sum_{i=1}^{N} L_{\rho_i}(\boldsymbol{x}, \delta_i, \boldsymbol{u}_i, \boldsymbol{v}_i, \boldsymbol{h}_i, q_i; \boldsymbol{\lambda}_i, \boldsymbol{\mu}_i, \nu_i), \tag{6}$$

where

$$L_{\rho_i}(\boldsymbol{x}, \delta_i, \boldsymbol{u}_i, \boldsymbol{v}_i, \boldsymbol{h}_i, q_i; \boldsymbol{\lambda}_i, \boldsymbol{\mu}_i, \nu_i) = w_i \left(\frac{1}{2}\|\boldsymbol{x} - \boldsymbol{a}_i\|^2 - \boldsymbol{v}_i^T(\boldsymbol{x} - \boldsymbol{a}_i) + \boldsymbol{h}_i^T(\boldsymbol{x} - \boldsymbol{a}_i) - q_i + \frac{1}{2}\delta_i^2 \right) + \boldsymbol{\lambda}_i^T(d_i\boldsymbol{u}_i - \boldsymbol{v}_i) + \boldsymbol{\mu}_i^T(\delta_i\boldsymbol{u}_i - \boldsymbol{h}_i) + \nu_i(d_i\delta_i - q_i) + \frac{\rho_i}{2}\|d_i\boldsymbol{u}_i - \boldsymbol{v}_i\|^2 + \frac{\rho_i}{2}\|\delta_i\boldsymbol{u}_i - \boldsymbol{h}_i\|^2 + \frac{\rho_i}{2}(d_i\delta_i - q_i)^2 + i_{\mathcal{B}_i}(\boldsymbol{u}_i),$$

with $i_{\mathcal{B}_i}(\boldsymbol{u}_i)$ denoting the indicator function of the unit closed ball $\mathcal{B}_i = \{\boldsymbol{u}_i \in \mathbb{R}^s : \|\boldsymbol{u}_i\| \leq 1\}$ and $\boldsymbol{\lambda}_i$, $\boldsymbol{\mu}_i$, and ν_i are dual variables, also known as Lagrange multipliers, which represent the sensitivity of the objective function for marginal perturbation of a constraint at the optimal point [30, Ch. 5]. The name augmented Lagrangian comes from the fact that in (6) one has the standard Lagrangian which is augmented by the quadratic penalty term, i.e., its penalty multiplier function is built in the form $\varphi(\boldsymbol{c}(\xi)) = \boldsymbol{\alpha}^T \boldsymbol{c}(\xi) + \frac{\tau}{2}\|\boldsymbol{c}(\xi)\|^2$, for some variable ξ, set of constraints $c_i(\xi)$, Lagrange multipliers α_i, and a penalty value τ.

The augmented Lagrangian in (6) is strongly convex in any of the variables for a fixed octet composed of the remaining variables. Hence, every minimization step of the ADMM (which comprises minimizing (6) in an alternating fashion for each primal variable, followed by an update of multipliers) results in a well-defined minimization of a strongly convex function for each primal step. This is done by generating the sequence $(\boldsymbol{x}^{(t)}, \delta^{(t)}, \boldsymbol{u}^{(t)}, \boldsymbol{v}^{(t)}, \boldsymbol{h}^{(t)}, q^{(t)}; \boldsymbol{\lambda}^{(t)}, \boldsymbol{\mu}^{(t)}, \nu^{(t)})$, with $t \in \mathbb{N}$, according to

$$\hat{\boldsymbol{x}}^{(t+1)} = \arg\min_{\boldsymbol{x}} L_\rho(\boldsymbol{x}, \hat{\boldsymbol{\delta}}^{(t)}, \hat{\boldsymbol{u}}^{(t)}, \hat{\boldsymbol{v}}^{(t)}, \hat{\boldsymbol{h}}^{(t)}, \hat{\boldsymbol{q}}^{(t)}; \hat{\boldsymbol{\lambda}}^{(t)}, \hat{\boldsymbol{\mu}}^{(t)}, \hat{\boldsymbol{\nu}}^{(t)}),$$

$$\hat{\delta}_i^{(t+1)} = \arg\min_{\delta_i} L_{\rho_i}(\hat{\boldsymbol{x}}^{(t+1)}, \delta_i, \hat{\boldsymbol{u}}_i^{(t)}, \hat{\boldsymbol{v}}_i^{(t)}, \hat{\boldsymbol{h}}_i^{(t)}, \hat{q}_i^{(t)}; \hat{\boldsymbol{\lambda}}_i^{(t)}, \hat{\boldsymbol{\mu}}_i^{(t)}, \hat{\nu}_i^{(t)}),$$

$$\hat{u}_i^{(t+1)} = \arg\min_{u_i} L_{\rho_i}(\hat{\boldsymbol{x}}^{(t+1)}, \hat{\delta}_i^{(t+1)}, \boldsymbol{u}_i, \hat{\boldsymbol{v}}_i^{(t)}, \hat{\boldsymbol{h}}_i^{(t)}, \hat{q}_i^{(t)}; \hat{\boldsymbol{\lambda}}_i^{(t)}, \hat{\boldsymbol{\mu}}_i^{(t)}, \hat{\nu}_i^{(t)}),$$

$$\hat{v}_i^{(t+1)} = \arg\min_{v_i} L_{\rho_i}(\hat{\boldsymbol{x}}^{(t+1)}, \hat{\delta}_i^{(t+1)}, \hat{\boldsymbol{u}}_i^{(t+1)}, \boldsymbol{v}_i, \hat{\boldsymbol{h}}_i^{(t)}, \hat{q}_i^{(t)}; \hat{\boldsymbol{\lambda}}_i^{(t)}, \hat{\boldsymbol{\mu}}_i^{(t)}, \hat{\nu}_i^{(t)}),$$

$$\hat{\boldsymbol{h}}_i^{(t+1)} = \arg\min_{\boldsymbol{h}_i} L_{\rho_i}(\hat{\boldsymbol{x}}^{(t+1)}, \hat{\delta}_i^{(t+1)}, \hat{\boldsymbol{u}}_i^{(t+1)}, \hat{\boldsymbol{v}}_i^{(t+1)}, \boldsymbol{h}_i, \hat{q}_i^{(t)}; \hat{\boldsymbol{\lambda}}_i^{(t)}, \hat{\boldsymbol{\mu}}_i^{(t)}, \hat{\nu}_i^{(t)}),$$

$$\hat{q}_i^{(t+1)} = \arg\min_{q_i} L_{\rho_i}(\hat{\boldsymbol{x}}^{(t+1)}, \hat{\delta}_i^{(t+1)}, \hat{\boldsymbol{u}}_i^{(t+1)}, \hat{\boldsymbol{v}}_i^{(t+1)}, \hat{\boldsymbol{h}}_i^{(t+1)}, q_i; \hat{\boldsymbol{\lambda}}_i^{(t)}, \hat{\boldsymbol{\mu}}_i^{(t)}, \hat{\nu}_i^{(t)}),$$

for $i = 1, \ldots, N$, while the updates of the multipliers come from the derivative of the penalty multiplier function with respect to its corresponding constraint. Hence, each of the local optimization problems can be solved by simply computing the gradient with respect to the relevant primal variable and setting it to zero. This leads to

$$\hat{\boldsymbol{x}}^{(t+1)} = \sum_{i=1}^{N} w_i \left(\boldsymbol{a}_i + \hat{\boldsymbol{v}}_i^{(t)} - \hat{\boldsymbol{h}}_i^{(t)}\right), \tag{7a}$$

$$\hat{\delta}_i^{(t+1)} = \frac{\rho_i d_i \hat{q}_i^{(t)} + \rho_i (\hat{\boldsymbol{u}}_i^{(t)})^T \hat{\boldsymbol{h}}_i^{(t)} - d_i \hat{\nu}_i^{(t)} - (\hat{\boldsymbol{u}}_i^{(t)})^T \hat{\boldsymbol{\mu}}_i^{(t)}}{1 + \rho_i + \rho_i d_i^2}, \tag{7b}$$

$$\hat{\boldsymbol{u}}_i^{(t+1)} = \frac{\boldsymbol{\beta}_i}{\max\{1, \|\boldsymbol{\beta}_i\|\}}, \tag{7c}$$

$$\hat{\boldsymbol{v}}_i^{(t+1)} = \frac{\hat{\boldsymbol{x}}^{(t+1)} - \boldsymbol{a}_i + \hat{\boldsymbol{\lambda}}_i^{(t)} + \rho_i d_i \hat{\boldsymbol{u}}_i^{(t+1)}}{\rho_i}, \tag{7d}$$

$$\hat{\boldsymbol{h}}_i^{(t+1)} = \frac{-\hat{\boldsymbol{x}}^{(t+1)} + \boldsymbol{a}_i + \hat{\boldsymbol{\mu}}_i^{(t)} + \rho_i \hat{\delta}_i^{(t+1)} \hat{\boldsymbol{u}}_i^{(t+1)}}{\rho_i}, \tag{7e}$$

$$\hat{q}_i^{(t+1)} = \frac{\rho_i d_i \hat{\delta}_i^{(t+1)} \hat{\nu}_i^{(t)} + 1}{\rho_i}, \tag{7f}$$

$$\hat{\boldsymbol{\lambda}}_i^{(t+1)} = \hat{\boldsymbol{\lambda}}_i^{(t)} + \rho_i \left(d_i \hat{\boldsymbol{u}}_i^{(t+1)} - \hat{\boldsymbol{v}}_i^{(t+1)}\right), \tag{7g}$$

$$\hat{\boldsymbol{\mu}}_i^{(t+1)} = \hat{\boldsymbol{\mu}}_i^{(t)} + \rho_i \left(\hat{\delta}_i^{(t+1)} \hat{\boldsymbol{u}}_i^{(t+1)} - \hat{\boldsymbol{h}}_i^{(t+1)}\right), \tag{7h}$$

$$\hat{\nu}_i^{(t+1)} = \hat{\nu}_i^{(t)} + \rho_i \left(d_i \hat{\delta}_i^{(t+1)} - \hat{q}_i^{(t+1)}\right), \tag{7i}$$

where

$$\boldsymbol{\beta}_i = \frac{\rho_i \hat{\delta}_i^{(t+1)} \hat{\boldsymbol{h}}_i^{(t)} + \rho_i d_i \hat{\boldsymbol{v}}_i^{(t)} - \hat{\delta}_i^{(t+1)} \hat{\boldsymbol{\mu}}_i^{(t)} - d_i \hat{\boldsymbol{\lambda}}_i^{(t)}}{\rho_i d_i^2 + \rho_i (\hat{\delta}_i^{(t+1)})^2},$$

and the update of the multipliers (7g)–(7i) just boils down to the sum of the previous value of the multiplier and the product of the penalty term multiplied with the value of the constraint in the current iteration. The scheme in (7) is referred to as WADMM in the following text.

B. Attacker Detection

Even though the proposed algorithm directly returns the estimated attack intensity of each anchor through (7b) as one of its outputs, one still needs to come up with a scheme in order to identify an anchor as genuine or malicious. For this purpose, the generalized likelihood ratio test (GLRT) is employed in this work. GLRT scheme is founded on discernment between two possible hypotheses:

$$H_0 : d_{i,k} = \|\boldsymbol{x} - \boldsymbol{a}_i\| + n_{i,k},$$
$$H_1 : d_{i,k} = \|\boldsymbol{x} - \boldsymbol{a}_i\| + \delta_i + n_{i,k}, \quad \delta_i \neq 0,$$

in which one assumes absence (H_0) and presence (H_1) of a malicious attacker. From these two hypotheses, the respective likelihood functions are defined as

$$p(\boldsymbol{d}_i|H_0) = \frac{1}{(2\pi\sigma^2)^{\frac{K}{2}}} \exp\left\{\sum_{k=1}^{K} \frac{(d_{i,k} - \|\boldsymbol{x} - \boldsymbol{a}_i\|)^2}{2\sigma^2}\right\}, \tag{9a}$$

$$p(\boldsymbol{d}_i|H_1) = \frac{1}{(2\pi\sigma^2)^{\frac{K}{2}}} \exp\left\{\sum_{k=1}^{K} \frac{(d_{i,k} - \|\boldsymbol{x} - \boldsymbol{a}_i\| - \delta_i)^2}{2\sigma^2}\right\}, \tag{9b}$$

where $\boldsymbol{d}_i$ is the vector assembled of K distance samples for each anchor i.

Then, applying the Neyman-Pearson theorem [31, Ch. 3] and taking advantage of (9a) and (9b) yields

$$\frac{p\left(\boldsymbol{d}_i|\widehat{\delta}_i,\widehat{\sigma},H_1\right)}{p\left(\boldsymbol{d}_i|\widehat{\sigma},H_0\right)} \underset{H_1}{\overset{H_0}{\lessgtr}} \gamma, \tag{10}$$

where γ denotes a threshold, and

$$\widehat{\delta}_i = \frac{1}{K}\sum_{k=1}^{K}\left(d_{i,k} - \|\hat{\boldsymbol{x}} - \boldsymbol{a}_i\|\right), \tag{11a}$$

$$\widehat{\sigma} = \sqrt{\frac{1}{K-1}\sum_{i=1}^{N}\sum_{k=1}^{K}\left(d_{i,k} - \|\hat{\boldsymbol{x}} - \boldsymbol{a}_i\| - \widehat{\delta}_i\right)^2}. \tag{11b}$$

respectively denote the ML estimate of the attack intensity for each link i and the ML estimate of the noise standard deviation [28, Ch. 7].

By plugging in (9a) and (9b) into (10) and applying some simple algebraic manipulations, the GLRT detection scheme reduces to

$$\left|\widehat{\delta}_i\right| \underset{H_1}{\overset{H_0}{\lessgtr}} \sqrt{\frac{2\widehat{\sigma}^2\ln(\gamma)}{K}}. \tag{12}$$

According to [31, Ch. 3], the probability of false alarm is defined as

$$\begin{aligned} P_{FA} &= P\left(H_1|\,H_0\right) \\ &= P\left(T_i > \sqrt{\frac{2\sigma^2\ln(\gamma)}{K}}\,\middle|\,H_0\right) = Q\left(\sqrt{2\ln(\gamma)}\right), \end{aligned} \tag{13}$$

where

$$T_i = \frac{1}{K}\sum_{k=1}^{K}\left(d_{i,k} - \|\boldsymbol{x} - \boldsymbol{a}_i\|\right),$$

i.e., $T_i \sim \mathcal{N}(0, \frac{\sigma^2}{K})$, under the hypothesis H_0. Thus, for a fixed value of P_{FA} in (13), it is straightforward to calculate the value of the threshold γ in order to solve (12).

Finally, to conclude this section, we summarize the generalized version of the proposed method in a universal setting as a pseudo-code in Algorithm 1.

Algorithm 1: Pseudo Code of WADMM Algorithm.

Require: $\boldsymbol{a}_i,\ d_{i,k},\ 1 \le i \le N,\ 1 \le k \le K,\ I_{max},\ \epsilon$
Initialization: Initialize all variables randomly and set $t \leftarrow 0$
`//Update all variables`
while $t \le I_{max}$ & $\|\hat{\boldsymbol{x}}^{(t+1)} - \hat{\boldsymbol{x}}^{(t)}\| > \epsilon$ **do**
  Update all variables according to (7)
  Set $t \leftarrow t+1$
end while
`//Obtain final location estimate`
$\hat{\boldsymbol{x}} \leftarrow \hat{\boldsymbol{x}}^{(t)}$
`//Estimate attack intensity at` i
$\widehat{\delta}_i \leftarrow$ (11a)
`//Estimate noise STD`
$\widehat{\sigma} \leftarrow$ (11b)
`//Detect attackers`
if $\left|\widehat{\delta}_i\right| > \sqrt{\frac{2\widehat{\sigma}^2\ln(\gamma)}{K}}$ **then**
  Classify anchor i as malicious
else
  Classify anchor i as genuine
end if

IV. Performance Assessment

This section assesses the overall performance of the proposed solution via numerical results. First, it gives a brief overview of all considered algorithms and analyzes their computational complexity, after which, localization and attacker detection performance analyses in a simulation and experimental environments follow. The section is concluded by a brief discussion of the proposed solution.

A. Analysis of the Computational Complexity

Table I lists the existing algorithms that are considered here as the state-of-the-art solutions[1] for comparison with the proposed one. It provides a summary of their main characteristics, together with their worst-case computational complexity and average running time. The table shows that some existing works designed their solution for a specific type of attack and that some of them require additional information beforehand in order to operate (e.g., WLS requires knowledge about the noise standard deviation, while R-GTRS requires knowledge about the upper bound on the magnitude of the attack intensity). Furthermore, Table I exhibits that the asymptotic computational complexity of all considered approaches is linear in N. The only difference in their computational burden is due their iterative nature, given that LC-GTRS and R-GTRS solve the problem via bisection (and B_{max} denotes the maximum number of iterations), while LN-1, LN-1E and WADMM use ADMM approach to reach their final solution (with k_{ADMM} and I_{max} denoting their maximum number of iterations). Note that LC-GTRS and LN-1E require an additional localization step after they "clean" the measurements from the *malicious* anchors. Lastly, it is also worth mentioning that the average running times were obtained in the scenario where $N = 30$, $\sigma = 15$ (m) and $\Delta = 20$ (m) for $M_c = 1000$ runs for both uncoordinated (UC) and coordinated (C) attacks, on the computer with the following characteristics: CPU Intel(R) Core(TM) i5-1135G7 @2.4 GHz and 16 GB RAM. The results in Table I show that the proposed algorithm requires the highest

[1] Note that the secure WLS (SWLS) method described in [20] is omitted here for comparison. The reason is that it is designed for RSS-based localization, where non-linear relationship between distance and RSS was exploited and its generalization to a common range-based approach is not straightforward. WLS in [18] (with GLRT for detection) is used instead.

TABLE I
BRIEF SUMMARY OF THE CONSIDERED ALGORITHMS

Algorithm	Type of attack	Additional Requirements	Complexity	Running time (s)
WADMM in Section III	UC & C	N/A	$\mathcal{O}(I_{max} \times N)$	0.25
WLS in [18]	UC	Knowledge about σ	$\mathcal{O}(N)$	0.002
LC-GTRS in [21]	UC	N/A	$2 \times \mathcal{O}(B_{max} \times N)$	0.05
LN-1 [20]	UC & C	N/A	$\mathcal{O}(k_{ADMM} \times N)$	0.03
LN-1E [20]	C	N/A	$2 \times \mathcal{O}(k_{ADMM} \times N)$	0.05
R-GTRS [22]	UC	Knowledge about Δ ($\lvert\delta_i\rvert \leq \Delta$)	$\mathcal{O}(B_{max} \times N)$	0.003

TABLE II
MAIN PARAMETERS FOR COMPUTER SIMULATIONS

Parameter	Designation	Value
True location of anchor i	$\boldsymbol{a}_i$	Random in $[-B;\, B] \times [-B;\, B]$
True location of the target	$\boldsymbol{x}$	Random in $[-B;\, B] \times [-B;\, B]$
Number of anchors	N	Variable
Maximum number of malicious anchors	N_M	$\frac{N}{2}$
Standard deviation of measurement noise (m)	σ	15
Area border length (m)	B	50
Maximum attack intensity (m)	Δ	Variable
Attack intensity of anchor i	δ_i	$\sim \pm\mathcal{E}(\mathcal{U}[0, \Delta])$
Number of attacks in a fixed topology	N_A	50
Number of measurement samples taken	K	10
Probability of false alarm	P_{FA}	0.1
Threshold in (10)	γ	$\exp\left\{\frac{1}{8}Q^{-1}(P_{FA})^2\right\}$
Maximum number of iterations	I_{max}	1000
Initial values of variables in (7)	Various	Random $[-B;\, B] \times [-B;\, B]$

average running time, but even so, all considered algorithms seem suitable for real-time implementation.

B. Localization and Detection Performance

In all presented results hereafter, every node was deployed randomly $N_D = 1000$ times in a square area with edge length of 100 meters. All measurements[2] were generated according to (1), where $K = 10$ measurement samples were considered. Moreover, at most half of all N anchors (chosen randomly) were considered as malicious $N_A = 50$ times in each node deployment. Note that attacks were performed independently by each malicious anchor, following 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. The proposed solution was executed with $I_{max} = 1000$. The main simulation parameters are summarized in Table II.

Although Table I shows that some existing solutions were specifically designed for a particular type of attack, since one cannot know under what type of attack (uncoordinated or coordinated) the network is beforehand, this section analyzes the performance of the considered algorithms in both scenarios. In the case where the authors of the considered existing works provided alternatives specifically for one of these setting, those solutions were used for comparison (e.g., WLS in [18] and LN-1E in [20] were only considered in uncoordinated and coordinated scenario, respectively); otherwise, the proposed methods were tested in both settings. Regardless, the main criteria used for evaluating localization accuracy are 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 Monte Carlo, $M_c = N_D \times N_A$, run, BIAS, defined as $\text{BIAS} = \|\sum_{m=1}^{M_c} \frac{(\boldsymbol{x}_m - \widehat{\boldsymbol{x}}_m)}{M_c}\|_1$, with $\|\bullet\|_1$ denoting the l_1 norm, and cumulative distribution function (CDF) of the localization error (LE), defined as $\text{LE}_m = \|\boldsymbol{x}_m - \widehat{\boldsymbol{x}}_m\|$. In terms of detection accuracy, the main performance metrics are the probability of correct detection, P_{CD}, and the probability of false detection, P_{FD}. It is worth mentioning that the probability of false alarm was set to $P_{F_A} = 0.1$, in order to compute the threshold in (13).

Fig. 2 illustrates the performance comparison of the considered schemes in an uncoordinated attack scenario for different values of N and fixed $\sigma = 15$ (m) and $\Delta = 20$ (m). Fig. 2(a) shows that the localization error of all algorithms reduces with the increase of N, as foreseen, since the maximum number of malicious anchors is at most $\frac{N}{2}$ and adding more anchors eventually results in adding more genuine devices into the network. It also shows that the proposed solution outperforms significantly the existing ones, lowering the localization error for at least 1 m for any N in comparison with the best existing solution in any setting. Fig. 2(b) exhibits that the BIAS (m) of the proposed solution is among the lowest of all considered estimators. Moreover, Fig. 2(c) and (d) study the detection performance of all algorithms.[3] Interestingly, in the considered scenario, it seems that all algorithms get saturated practically immediately in terms of the correct detection, and increasing N brings no substantial improvements. These results indicate that there might be an upper bound on the achievable P_{CD} performance (a bit above 50%) that no existing solution is able to exceed for any considered N. Nevertheless, the proposed estimator is competitive in comparison with the existing ones and performs relatively close to the achievable upper bound. Finally, it is also interesting to see the detection performance in terms of false detection, i.e., how many times does an estimator mistakenly tags a genuine anchor as a malicious one. It can be seen from Fig. 2(d) that all solutions slightly lower P_{FD} with the increase of N, which is in concordance with the localization results presented in Fig. 2(a). The proposed algorithm exhibits the least P_{FD} for all considered N, followed closely by R-GTRS method. Interestingly, by observing both the results presented in Fig. 2(c) and (d), one can conclude that LC-GTRS and WLS are

[2]Even though the attack intensity of each malicious node is considered consistent in one simulation run, given that the observations are constructed on top of a noisy measurement model in (1), the resulting attack realizations are actually impaired.

[3]Note that, in its original form, the LN-1 algorithm in [20] only solves the localization problem in a single step. However, since it is used as a base on top of which LN-1E is built, by applying plane fitting and K-means clustering to detect the attackers, after which another LN-1 iteration is employed, but this time exploiting only *genuine* anchors, the same detection principle was employed here to accomplish LN-1's detection.

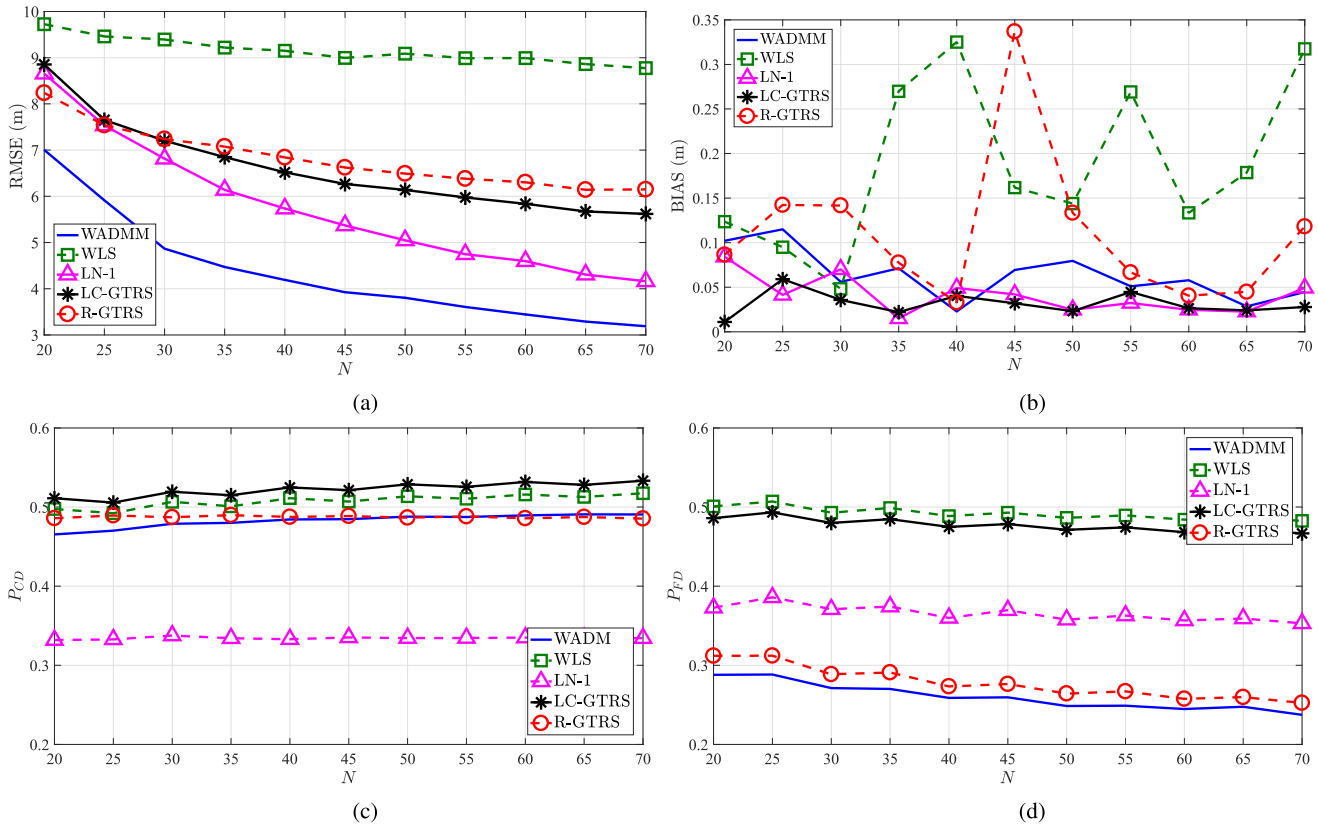

Fig. 2. Performance comparison for variable N in an uncoordinated attack scenario, when $\sigma = 15$ (m) and $\Delta = 20$ (m). (a) RMSE (m) versus N illustration (b) BIAS (m) versus N illustration (c) P_{CD} versus N illustration(d) P_{FD} versus N illustration.

basically "flip-a-coin" detection methods, since they practically identify all anchors as malicious, i.e., $P_{CD} + P_{FD} \approx 1$ for these methods.

Fig. 3 illustrates the performance comparison of the considered schemes in a coordinated attack scenario for different values of Δ (m) and fixed $N = 50$ and $\sigma = 15$ (m). Naturaly, Fig. 3(a) shows that all considered algorithms suffer a deterioration in localization accuracy with the increase of Δ (m), since every successful malicious deed leads to a greater mistake in localization estimation. Still, the proposed solution outperforms the existing ones for practically all considered Δ (m), although R-GTRS and LN-1 solutions are competitive for small-to-medium Δ (m). In terms of BIAS (m), Fig. 3(b) corroborates that the proposed method is one of the least biased ones. Regarding detection performance in the considered scenario, the proposed algorithms exhibit the lowest P_{CD} performance, but likewise the lowest P_{FD} performance. These results indicate that many times (especially for low Δ (m)) the proposed solution does not detect any attackers. Nonetheless, these results do not influence its localization performance, given that they come as a consequence of the final localization solution, unlike LC-GTRS and LN-1E that require an extra iteration with only *genuine* anchors. Similar as in the uncoordinated scenario, LC-GTRS is a "flip-a-coin" detection method.

Figs. 4 and 5 illustrate the effect of the proportion of the number of malicious anchors, N_M, to the total number of anchors, N, on the localization error in the uncoordinated and coordinated scenarios, respectively. As one can see from these figures, the proposed solution outperforms the existing ones for any considered proportion of the malicious anchors in terms of localization error and shows the lowest P_{FD}, while it exhibits somewhat lower P_{CD} performance.

Fig. 6 illustrates the CDF versus LE (m) performance comparison in the two considered scenarios, for fixed values of $N = 50$, $\sigma = 15$ (m), and $\Delta = 20$ (m). From Fig. 6, it is obvious that the coordinated scenario is more demanding than the uncoordinated one, given that all methods suffer deterioration in their localization accuracy. Still, in both uncoordinated and coordinated scenarios, it can be seen that the proposed estimator outperforms the existing solutions, with a higher emphasis in uncoordinated setting.

C. Experimental Validation

This section presents an experimental study that was carried out by using KIO Real Time Location System equipment [32], which follows the IEEE802.15.4-2011-UWB communication standard and extracts the distance information from the time of flight measurements. In Fig. 7, the devices used in the experiment are presented: the target (on the left) and an anchor (on the right). The KIO kit included three anchors and a tag (target), which was used repeatedly at various locations in order to produce a realistic

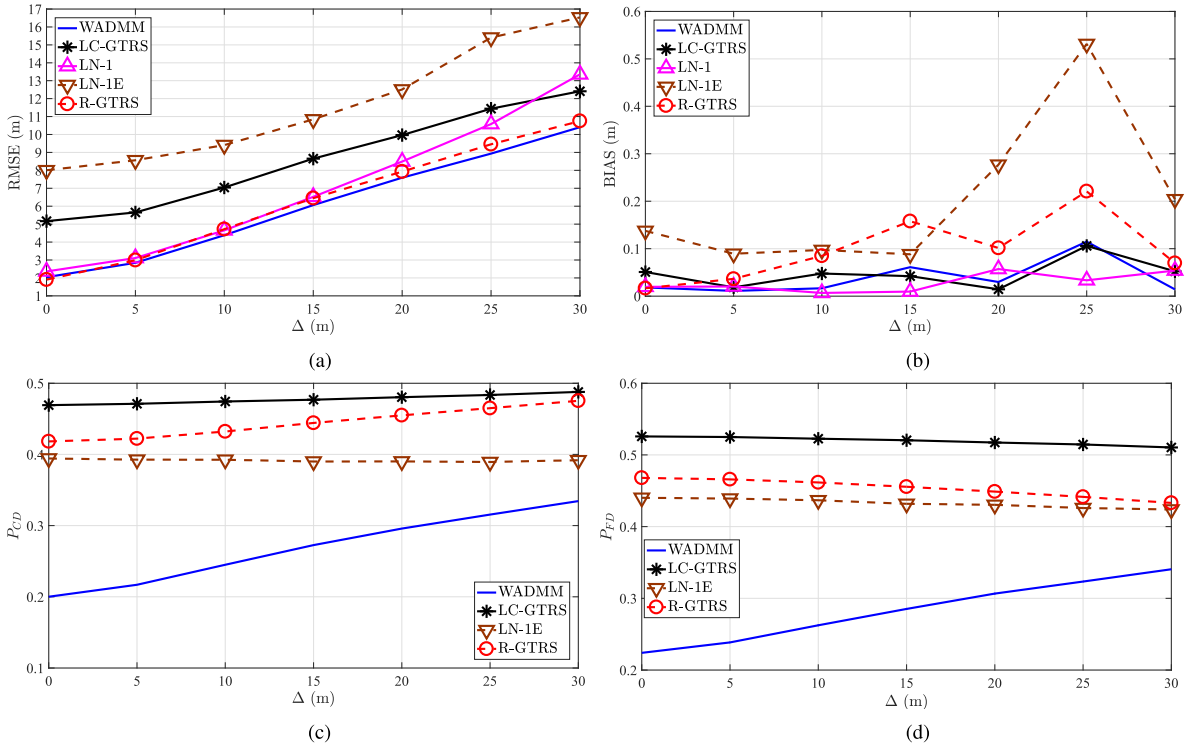

Fig. 3. Performance comparison for variable Δ in a coordinated attack scenario, when $N = 50$ and $\sigma = 15$ (m). (a) RMSE (m) versus Δ (m) illustration (b) BIAS (m) versus Δ (m) illustration (c) P_{CD} versus Δ (m) illustration (d) P_{FD} versus Δ (m) illustration.

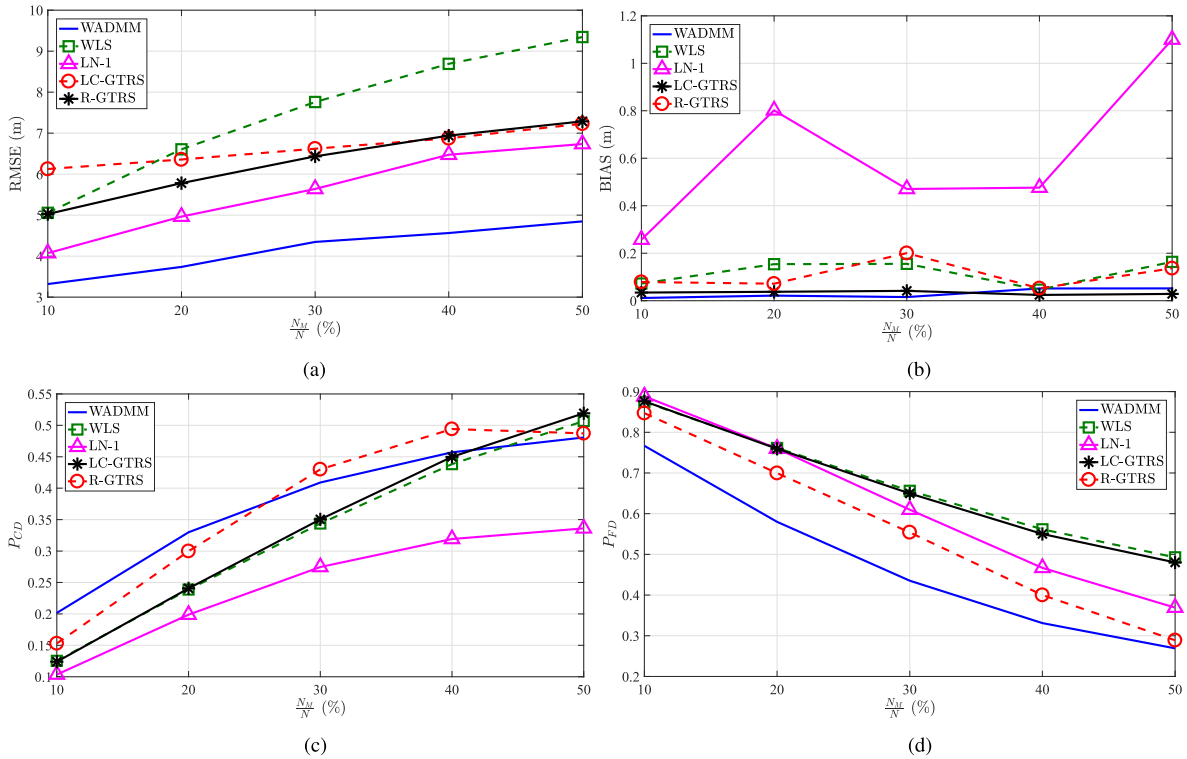

Fig. 4. Performance comparison for variable $\frac{N_M}{N}$ (%) in the considered uncoordinated scenario, when $N = 30$, $\sigma = 15$ (m) and $\Delta = 20$ (m). (a) RMSE (m) versus $\frac{N_M}{N}$ (%) illustration (b) BIAS (m) versus $\frac{N_M}{N}$ (%) illustration (c) P_{CD} versus $\frac{N_M}{N}$ (%) illustration (d) P_{FD} versus $\frac{N_M}{N}$ (%) illustration.

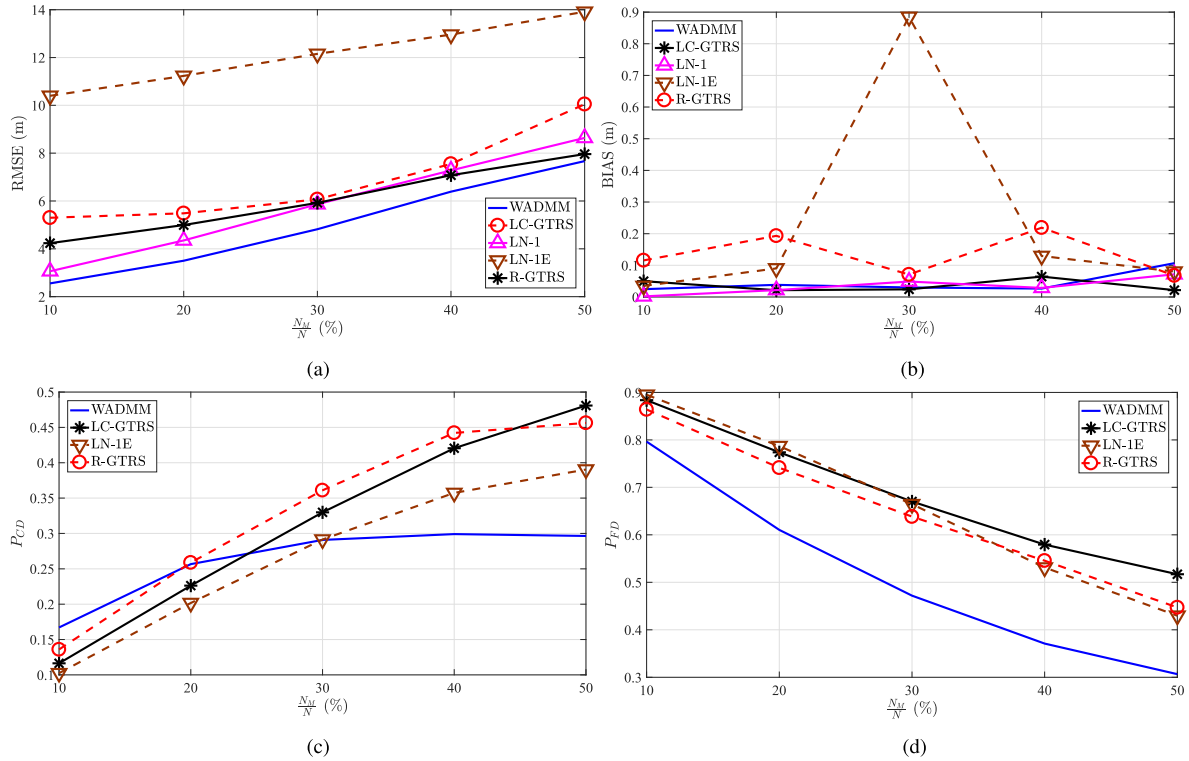

Fig. 5. Performance comparison for variable $\frac{N_M}{N}$ (%) in the considered coordinated scenario, when $N = 50$, $\sigma = 15$ (m) and $\Delta = 20$ (m). (a) RMSE (m) versus $\frac{N_M}{N}$ (%) illustration (b) BIAS (m) versus $\frac{N_M}{N}$ (%) illustration (c) P_{CD} versus $\frac{N_M}{N}$ (%) illustration (d) P_{FD} versus $\frac{N_M}{N}$ (%) illustration.

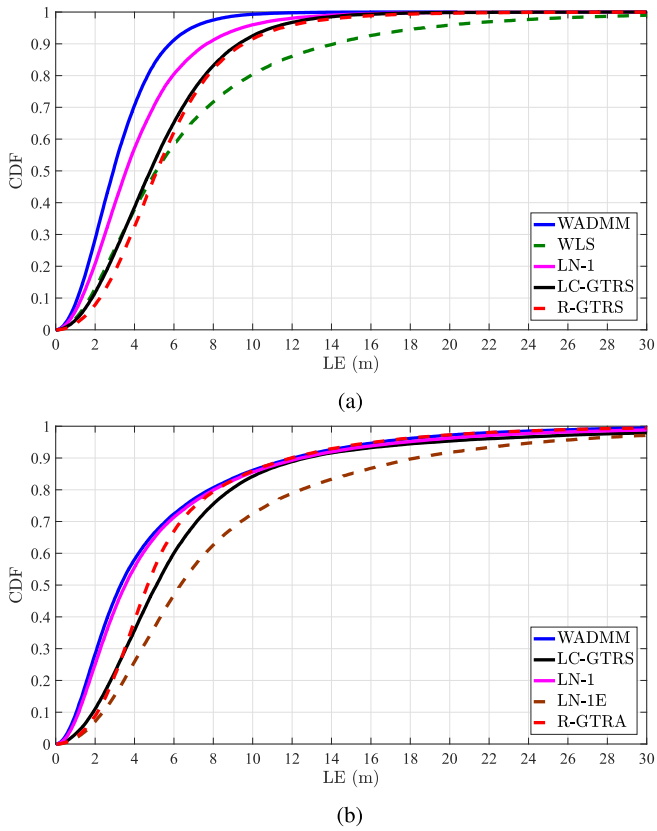

Fig. 6. CDF versus LE (m) illustration, when $N = 50$, $\sigma = 15$ (m), and $\Delta = 20$ (m). (a) Uncoordinated scenario (b) Coordinated scenario.

Fig. 7. Equipment used for the experiment: target (left) and anchor (right).

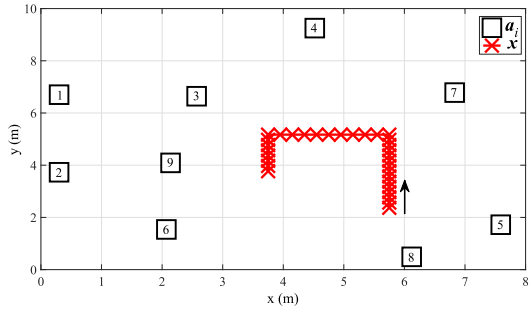

Fig. 8. Experimental set-up with 9 anchors (black squares) and 32 targets (red circles).

indoor scenario, as shown in Fig. 8. The measurement campaign was realized inside the Instituto Superior Técnico building at Taguspark campus, Oeiras, Portugal.

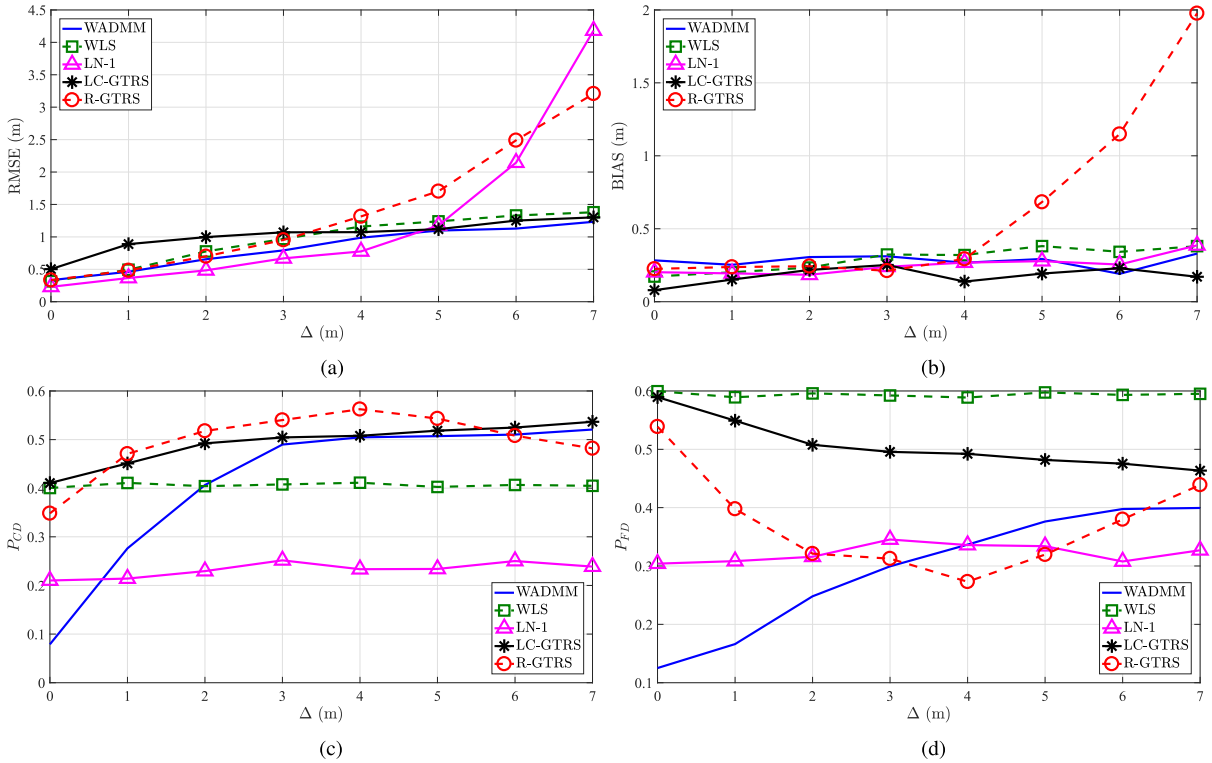

Fig. 9. Performance comparison for variable Δ (m) in the considered experimental uncoordinated attack scenario, when $N = 9$, $N_A = 20$ and $N_D = 32$. (a) RMSE (m) versus Δ (m) illustration. (b) BIAS (m) versus Δ (m) illustration. (c) P_{CD} versus Δ (m) illustration. (d) P_{FD} versus Δ (m) illustration.

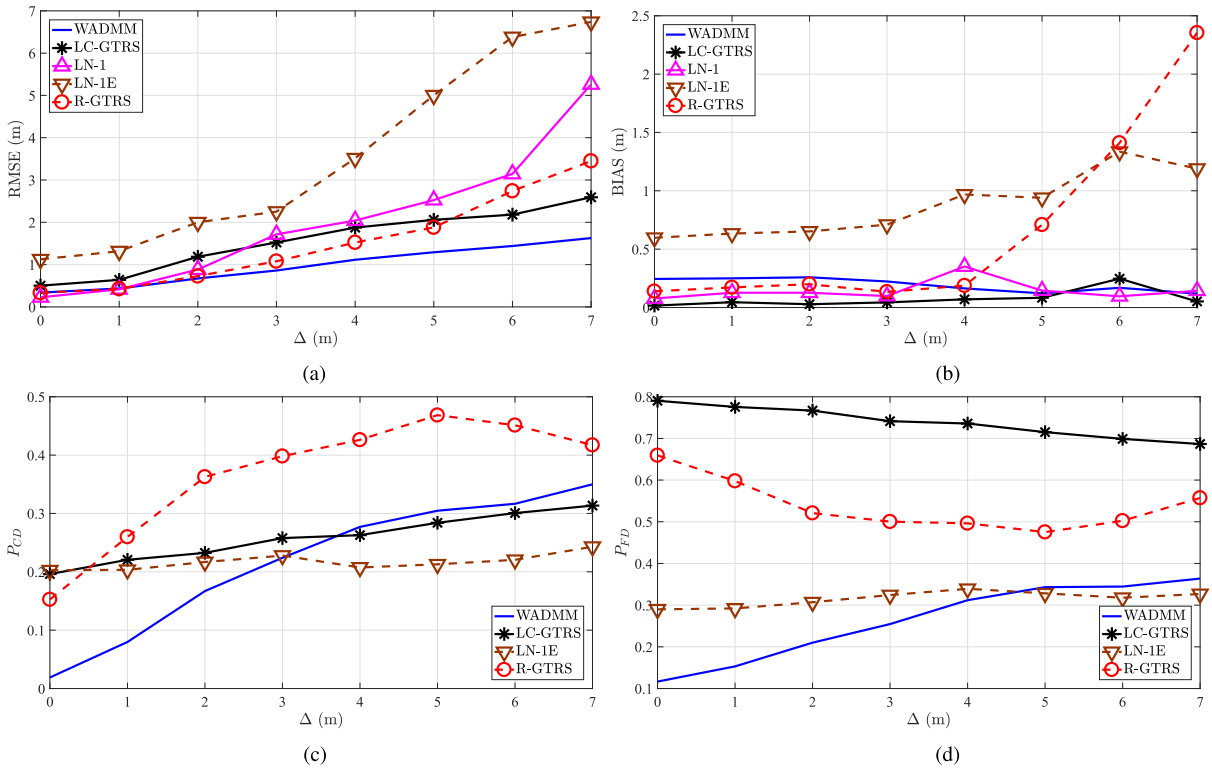

Fig. 10. Performance comparison for variable Δ (m) in the considered experimental coordinated attack scenario, when $N = 9$, $N_A = 20$ and $N_D = 32$. (a) RMSE (m) versus Δ (m) illustration. (b) BIAS (m) versus Δ (m) illustration. (c) P_{CD} versus Δ (m) illustration. (d) P_{FD} versus Δ (m) illustration.

After the data measurement campaign was performed, at most 4 anchors were randomly selected as corrupted and their malicious attacks were added posteriorly in the same manner as it was done in the computer simulation scenario explained in Section IV-B. Both uncoordinated and coordinated attack scenarios were considered and the results are presented in Figs. 9 and 10, respectively. The figures show that the proposed method performs significantly better than the existing ones for high attack intensities, while it matches the performance of the existing ones for low attack intensities.

D. Discussion

Even though the proposed approach outperforms the existing solutions in terms of localization accuracy in general, while achieving comparable success in attacker identification, it might be of interest to expose some of its limitations. Clearly, the proposed solution makes a hard decision regarding classification of an anchor as a genuine or malicious. However, it could be of interest to try to implement some kind of a soft decision, where anchors would be classified probabilistically and one could exploit these probabilities as weights to perhaps repeat the main procedure and accomplish further enhancement of its performance from both localization and detection perspectives. It is intuitively clear that the proposed method can endure malicious attacks of up to 50% of all anchors, especially in the case of coordinated attacks. However, this is a common limitation to all existing methods that might not be possible to surpass. Another particularity of the proposed solution is that it is executed iteratively. Hence, it might be possible in some settings that the proposed solution converges slowly enough to not reach its optimal value within the predefined maximum number of iterations, given the high degree of difficulty of the problem at hand and relatively high number of variables that are involved. Nevertheless, this issue could be circumvented by simply increasing the maximum number of iterations to give the algorithm enough time to converge.

V. Conclusion

This work presented an elegant ADMM approach to combat the localization problem in the presence of malicious attackers that try to spoof the localization process. The proposed approach is based on two main building blocks: 1) transforming the original unconstrained optimization problem into an equivalent, but smooth constrained problem via a variable splitting procedure; 2) addressing the derived constrained problem by exploiting the benefits of dual decomposition and augmented Lagrangian methods. Two types of spoofing attacks were under scrutiny, uncoordinated (in which every attacker acts independently) and coordinated (a set of attackers act in conjunction). Since one cannot know under which type of attack the network is beforehand, the proposed solution was tested in both settings in a simulation and an experimental environment, were it showed superior performance than the state-of-the-art methods in terms of localization accuracy. To distinguish between genuine and malicious devices, the proposed approach adopted GLRT and achieved competitive results in terms of correct detection in uncoordinated attack scenario, while somewhat lower detection success was achieved in a coordinated attack setting. At the same time, the new estimator accomplished significantly reduced false detection in both considered setting.

References

[1] Y. Zhong et al., "Empowering the V2X network by integrated sensing and communications: Background, design, advances, and opportunities," *IEEE Netw.*, vol. 36, no. 4, pp. 54–60, Jul./Aug. 2022.

[2] H. Zhou, C. She, Y. Deng, M. Dohler, and A. Nallanathan, "Learning for massive industrial Internet of Things," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 81–87, Aug. 2021.

[3] H. C. Yang and M. S. Alouini, "Data-oriented transmission in future wireless systems: Toward trustworthy support of advanced Internet of Things," *IEEE Veh. Technol. Mag.*, vol. 14, no. 3, pp. 78–83, Sep. 2019.

[4] L. U. Khan, Z. Han, W. Saad, E. Hossain, M. Guizani, and C. S. Hong, "Digital twin of wireless systems: Overview, taxonomy, challenges, and opportunities," *IEEE Commun. Surv. Tuts.*, vol. 24, no. 4, pp. 2230–2254, Oct.–Dec. 2022.

[5] J. I. D. O. Filho, A. Trichili, B. S. Ooi, M. S. Alouini, and K. N. Salama, "Toward self-powered Internet of Underwater Things devices," *IEEE Commun. Mag.*, vol. 58, no. 2, pp. 68–73, Jan. 2020.

[6] J. Yang, S. Jin, C.-K. Wen, X. Yang, and M. Matthaiou, "Fast beam training architecture for hybrid mmWave transceivers," *IEEE Trans. Veh. Technol.*, vol. 69, no. 3, pp. 2700–2715, Mar. 2020.

[7] T. A. Tsiftsis, C. Valagiannopoulos, H. Liu, A.-A. A. Boulogeorgos, and N. I. Miridakis, "Metasurface-coated devices: A new paradigm for energy-efficient and secure 6G communications," *IEEE Veh. Technol. Mag.*, vol. 17, no. 1, pp. 27–36, Mar. 2022.

[8] A. A. A. Boulogeorgos and A. Alexiou, "Coverage analysis of reconfigurable intelligent surface assisted THz wireless systems," *IEEE Open J. Veh. Technol.*, vol. 2, pp. 94–110, 2021.

[9] A.-A. A. Boulogeorgos, N. D. Chatzidiamantis, H. G. Sandalidis, A. Alexiou, and M. D. Renzo, "Cascaded composite turbulence and misalignment: Statistical characterization and applications to reconfigurable intelligent surface-empowered wireless systems," *IEEE Trans. Veh. Technol.*, vol. 71, no. 4, pp. 3821–3836, Apr. 2022.

[10] S. E. Trevlakis et al., "Localization as a key enabler of 6 G wireless systems: A comprehensive survey and an outlook," *IEEE Commun. Survey Tut.*, vol. 4, pp. 2733–2801, Oct. 2023.

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

[12] D. He, L. Cui, H. Huang, and M. Ma, "Design and verification of enhanced secure localization scheme in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 20, no. 7, pp. 1050–1058, Jul. 2009.

[13] 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.

[14] 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.

[15] J. Won and E. Bertino, "Robust sensor localization against known sensor position attacks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 2, pp. 2954–2967, Dec. 2019.

[16] 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 Trans. Commun.*, vol. 69, no. 7, pp. 4691–4703, Jul. 2021.

[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 Things J.*, vol. 8, no. 8, pp. 6878–6892, Apr. 2021.

[18] B. Mukhopadhyay, S. Srirangarajan, and K. Kar, "Robust range-based secure localization in wireless sensor networks," in *Proc. IEEE Glob. Commun. Conf.*, 2018, pp. 1–6.

[19] M. Beko and S. Tomic, "Towards secure localization in randomly deployed wireless networks," *IEEE Internet Things J.*, vol. 8, no. 24, pp. 17436–17448, Dec. 2021.

[20] 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.

[21] 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.
[22] S. Tomic and M. Beko, "A min-max optimization-based approach for secure localization in wireless networks," *IEEE Trans. Veh. Technol.*, early access, Oct. 16, 2023, doi: 10.1109/TVT.2023.3325063.
[23] 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.
[24] H. So, J. Jang, K. Lee, and J. Park, "Performance analysis of a COTS GPS receiver against spoofing attack and spoofing detection method using RAIM and a single authentic signal," *Trans. Jpn. Soc. Aeronautical Space Sci.*, vol. 60, no. 5, pp. 312–319, May 2017.
[25] 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, Feb. 2021.
[26] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *J. Secur. Admin.*, vol. 25, no. 2 pp. 19–27, 2002.
[27] M. Singh, P. Leu, A. Abdou, and S. Capkun, "UWB-ED: Distance enlargement attack detection in ultra-wideband," in *Proc. 28th USENIX Secur. Symp.*, 2019, pp. 73–88.
[28] S. M. Kay. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1993.
[29] J. M. Bioucas-Dias and M. A. T. Figueiredo, "Multiplicative noise removal using variable splitting and constrained optimization," *IEEE Trans. Image Process.*, vol. 19, no. 7, pp. 1720–1730, Jul. 2010.
[30] S. Boyd and L. Vanderberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge University Press, 2004.
[31] S. M. Kay. *Fundamentals of Statistical Signal Processing: Detection Theory*. Upper Saddle River, NJ, USA: Prentice-Hall, 1998.
[32] Precise "UWB-based real time location system," OU Eliko Tehnoloogia Arenduskeskus, Tallin, Estonia: [Online]. Available: http://www.eliko.ee/products/kio-rtls/

Slavisa Tomic received the M.S. degree in traffic engineering according to the postal traffic and telecommunications study program from the University of Novi Sad, Novi Sad, Serbia, in 2010, and the Ph.D. degree in electrical and computer engineering from the University Nova of Lisbon, Lisbon, Portugal, in 2017. He is currently an Assistant Professor with the Universidade Lusófona, Lisbon. 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, 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. 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. His research interests include the area of signal processing for wireless communications. He is 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 was the recipient of the 2008 IBM Portugal Scientific Award.