Visible Light Positioning in the Presence of Malicious LED Transmitters

Furkan Kokdogan, *Student Member, IEEE*, Sinan Gezici, *Senior Member, IEEE*

***Abstract*—We consider a visible light positioning system in which a receiver performs position estimation based on signals emitted from a number of light emitting diode (LED) transmitters. Each LED transmitter can be malicious and transmit at an unknown power level with a certain probability. A maximum likelihood (ML) position estimator is derived based on the knowledge of probabilities that LED transmitters can be malicious. In addition, in the presence of training measurements, decision rules are designed for detection of malicious LED transmitters, and based on detection results, various ML based location estimators are proposed. To evaluate the performance of the proposed estimators, Cramér-Rao lower bounds (CRLBs) are derived for position estimation in scenarios with and without a training phase. Moreover, an ML estimator is derived when the probabilities that the LED transmitters can be malicious are unknown. The performances of all the proposed estimators are evaluated via numerical examples and compared against the CRLBs.**

***Index Terms*– Visible light, estimation, localization, malicious LED transmitter, CRLB.**

I. Introduction

Recently, the usage of light emitting diodes (LEDs) as efficient lighting sources in indoor environments has become widespread due to their low power consumption, efficient illumination, and long life span compared to conventional light bulbs [2]. In addition to illumination, LEDs can also be utilized for communications and positioning. In particular, visible light positioning (VLP) has emerged as an attractive approach that provides accurate location information with low implementation complexity. In the literature, various position estimation algorithms are developed and theoretical accuracy limits are investigated for VLP systems thoroughly [3]–[6] (and references therein). Unlike in RF systems, position estimation based on received power measurements can achieve high accuracy in VLP systems [7]. Therefore, the received signal strength (RSS) parameter is commonly employed in VLP systems due to its low measurement cost. In [8], closed-form Cramér-Rao lower bound (CRLB) expressions are derived for location and orientation estimation based on the RSS measurements. In [9], a three-dimensional (3D) positioning approach that utilizes both RSS and angle-of-arrival (AOA) information is introduced for a single-input multiple-output (SIMO) visible light system. The authors in [10] propose a simultaneous position and orientation estimation (SPO) algorithm using RSS measurements in a multi-input multi-output (MIMO) VLP system. The CRLB is also derived to evaluate the performance of the proposed SPO estimator. In [11], deep learning is employed for joint 3D position and orientation estimation of a VLC receiver with a random orientation and an unknown emitting power based on RSS measurements. In [12], performance analysis of a VLP system, which uses an aperture-based receiver, is conducted. An estimator is proposed by utilizing both RSS and AOA information. Also, the CRLB is derived for assessing the performance of the proposed estimator.

In this work, we focus on a VLP system in which a visible light communication (VLC) receiver collects power measurements from signals coming from a number of LED transmitters for the purpose of localization. We also consider that the system is not completely secure and some of the LED transmitters can be malicious (controlled by a third party). Therefore, we aim to develop position estimation algorithms in the presence of malicious LED transmitters. Although various security issues in the physical layer have been investigated for VLC systems [13]–[22], there exists no such work for VLP systems in the literature. For example, [14] considers the presence of an eavesdropper and proposes a way of securing VLC links via friendly jammers. In addition, a robust beamforming approach is developed to maximize the worst-case secrecy rate in the presence of imperfect knowledge of eavesdropper's channel. In [17], a multiple-input single-output (MISO) VLC system is investigated in the presence of multiple eavesdroppers. The transmit beamformer and jamming precoder are optimized to improve communication secrecy. In [18], simultaneous beamforming and jamming is utilized for MISO VLC systems under the assumption of randomly located eavesdropper in order to enhance the physical layer security. The authors formulate an optimization problem with a focus on the signal-to-interference-plus-noise ratio for the legitimate link and solve it by a heuristic method. In [19], a physical layer security technique is proposed for VLC systems with the utilization of an intelligent mirror array. An achievable secrecy rate maximization problem is formulated for the proposed technique and optimal orientations of the mirrors are found. In addition, the studies in [20] and [21] focus on the calculation of the secrecy capacity for VLC systems in various scenarios. A comprehensive survey on physical layer security for VLC systems can be found in [22]. As an alternative approach, information theoretic learning criteria, such as minimum error entropy (MEE) and maximum correntropy criterion (MCC), can also be employed for parameter estimation in visible light

F. Kokdogan and S. Gezici are with the Department of Electrical and Electronics Engineering, Bilkent University, Ankara 06800, Turkey (e-mails: {kokdogan, gezici}@ee.bilkent.edu.tr).

Part of this work was presented at 2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), May 24-28, 2021 [1].

systems. For example, an MEE based channel estimator is proposed in [23] for massive MIMO VLC systems.

In RF systems, position estimation in wireless sensor networks in the presence of malicious nodes has been considered in various studies [24]–[33]. In [24], independent and collaborative Byzantine attacks are considered and two different schemes are proposed for mitigation of these attacks. In addition, the posterior CRLB is derived to characterize the performance of the wireless sensor network. In [25], an RSS based localization method is proposed in order to mitigate the impacts of Byzantine fault and non-line-of-sight (NLOS) bias on the positioning accuracy. In [26], coding-theory based mitigation approach schemes are discussed in the presence of malicious nodes in sensor networks.

Although the approaches developed for RF localization in the presence of malicious devices can be considered for VLP systems, specific analyses are required for VLP in the presence of malicious LED transmitters due to distinct operating characteristics and channel models of visible light systems. [4]. The main contributions and novelty of this manuscript can be summarized as follows:

- Position estimation problems in visible light systems in the presence of malicious LED transmitters are formulated for the first time in the literature.
- A maximum likelihood (ML) estimator is derived based on the knowledge of probabilities that LED transmitters can be malicious.
- In the presence of training measurements, decision rules (namely, generalized likelihood ratio tests) are developed for detection of malicious LED transmitters, and based on detection results, various ML based location estimators are derived.
- CRLB expressions are derived and used as benchmarks for scenarios with and without training measurements.
- An ML estimator is obtained for the case that the probabilities of the LED transmitters being malicious are unknown.

In addition, simulation results are presented to investigate the performance of the proposed algorithms and to compare them against each other and the CRLBs.

In the conference version of this study [1], the estimators in Section III, Section IV-A, and Section IV-B were presented. In this manuscript, we also provide the following extensions: (i) An alternative detection approach is proposed in Section IV-C by showing the existence of the uniformly most powerful (UMP) test under certain conditions. (ii) The CRLB expressions are derived under three different settings in Section V. (iii) For the case of unknown probabilities for malicious LED transmitters, the ML estimator is obtained in Section VII. (iv) More detailed simulation results are performed to investigate the effects of various system parameters on localization performance in Section VI.

The rest of the manuscript is organized as follows. The system model is discussed in Section II. In Section III, an ML estimator is derived based on the knowledge of the probabilities of LED transmitters being malicious. In Section IV, a training procedure is proposed for the detection of malicious LEDs, and estimators that utilize the training measurements are derived for two different scenarios. In Section V, theoretical limits, namely, the CRLBs, on the positioning accuracy are derived. Simulation results are presented and discussed in Section VI. In Section VII, an extension is provided for the case of unknown probabilities of LEDs being malicious. Finally, the concluding remarks are presented in Section IX.

II. System Model

Consider a VLP system with $N_{\rm L}$ LED transmitters at known locations denoted by $\boldsymbol{l}_{\rm T}^{i}$ for $i \in \{1,\ldots,N_{\rm L}\}$. The LED transmitters communicate with a VLC receiver, which aims to estimate its unknown location $\boldsymbol{l}_{\rm R}$ based on signals coming from the LED transmitters. The VLP system is not completely secure and it is possible that some of the LED transmitters can be hijacked by malicious third parties. The VLC receiver does not know which LED transmitters are malicious but it is aware of such a possibility. Namely, it is assumed that the VLC receiver knows the probabilities that the LED transmitters can be malicious. (Extensions to the case of unknown probabilities is provided in Section VII.)

The VLC receiver gathers power measurements from the LED transmitters for the purpose of localization, which are expressed as [34]

$$P_{{\rm R},i} = R_p\, P_{{\rm T},i}\, h_i(\boldsymbol{l}_{\rm R}) + \eta_i \tag{1}$$

for $i = 1,\ldots,N_{\rm L}$. In (1), R_p denotes the responsivity of the photo detector (PD) at the VLC receiver, $P_{{\rm T},i}$ is the transmit power of the ith LED transmitter, $h_i(\boldsymbol{l}_{\rm R})$ represents the channel coefficient between the VLC receiver and the ith LED transmitter, and η_i is zero-mean Gaussian noise with a variance of σ_i^2, which is independent of η_j for all $j \neq i$ [34]. It is assumed that a certain type of multiple access protocol, such as frequency-division or time-division multiple access [35]–[37], is employed so that the signals coming from different LED transmitters are processed separately and their power levels are measurement individually as in (1).

Let γ_i denote the probability that the ith LED transmitter is malicious. Then, the transmit power parameter in (1) is given by

$$P_{{\rm T},i} = \begin{cases} P_{{\rm M},i}\,, & \text{with probability } \gamma_i \\ P_{{\rm H},i}\,, & \text{with probability } 1-\gamma_i \end{cases} \tag{2}$$

where $P_{{\rm M},i}$ denotes the transmit power of the ith LED transmitter if it is malicious (i.e., controlled by a third party) and $P_{{\rm H},i}$ represents the transmit power of the ith LED transmitter if it is honest (i.e., not malicious). The parameters $\{P_{{\rm H},i}\}_{i=1}^{N_{\rm L}}$ are known by the VLC receiver since transmit power levels in case of honest LED transmitters are either reported to the VLC receiver or they are set beforehand for localization purposes. On the other hand, when an LED transmitter is malicious, it can change its transmit power level in order to degrade the localization performance of the VLP system. Therefore, $\{P_{{\rm M},i}\}_{i=1}^{N_{\rm L}}$ are modeled as unknown parameters. Also, it is assumed that each LED transmitter can be malicious or honest independently of the other LED transmitters.

Considering a line-of-sight scenario between each LED transmitter and the VLC receiver [4], [38], [39], the channel coefficients in (1) can be calculated as

$$h_i(\boldsymbol{l}_{\rm R}) = \frac{(m_i+1)A_{\rm R}\left[(\boldsymbol{l}_{\rm R}-\boldsymbol{l}_{\rm T}^i)^T\boldsymbol{n}_{\rm T}^i\right]^{m_i}(\boldsymbol{l}_{\rm T}^i-\boldsymbol{l}_{\rm R})^T\boldsymbol{n}_{\rm R}}{2\pi\left\|\boldsymbol{l}_{\rm R}-\boldsymbol{l}_{\rm T}^i\right\|^{m_i+3}} \tag{3}$$

where m_i is the Lambertian order for the ith LED transmitter, $A_{\rm R}$ is the area of the PD at the VLC receiver, and $\boldsymbol{n}_{\rm R}$ and $\boldsymbol{n}_{\rm T}^i$ represent the orientation vectors of the VLC receiver and the ith LED transmitter, respectively [40]. It is assumed that the VLC receiver knows the parameters $A_{\rm R}$, R_p, $\boldsymbol{n}_{\rm R}$, m_i, $\boldsymbol{l}_{\rm T}^i$, and $\boldsymbol{n}_{\rm T}^i$, and σ_i^2 [7], [39]. For example, the orientation of the VLC receiver ($\boldsymbol{n}_{\rm R}$) can be determined by a gyroscope and the LED parameters (m_i, $\boldsymbol{l}_{\rm T}^i$, and $\boldsymbol{n}_{\rm T}^i$) can be sent to the receiver via visible light communications [7]. It is noted that the channel coefficient $h_i(\boldsymbol{l}_{\rm R})$ in (3) is a nonlinear function of the parameter of interest, i.e., $\boldsymbol{l}_{\rm R}$.

Remark 1: As implied from the preceding system model, malicious LED transmitters modify the transmit power levels to degrade the localization performance of the VLP system. Even though a malicious third party can control an LED transmitter, it is not practical for it to change other LED parameters such as $\boldsymbol{l}_{\rm T}^i$, $\boldsymbol{n}_{\rm T}^i$, and m_i as their modification requires physical intervention to the system. For example, the modification of $\boldsymbol{l}_{\rm T}^i$ or $\boldsymbol{n}_{\rm T}^i$ requires a change in the location or the orientation of the ith LED transmitter. Similarly, the Lambertian order is fixed for a given LED model. On the other hand, the transmit power levels of the LEDs are controlled by the LED drivers (usually via a controller unit). Therefore, without any physical change to the system (such as changing the locations and orientations of the LEDs or replacing the LEDs), a malicious third party can change the transmit power levels by hacking the LED drivers to degrade the positioning accuracy of the VLP system.

Remark 2: The VLP system model considered in this work can be practical in the following cases: (i) While the transmit power level is known for a given LED transmitter under normal operating conditions (denoted by $P_{{\rm H},i}$ in (2)), there can occur situations in which an LED can fail and provide a different (and unknown) power level than the reported one [41]–[43]. With a more general perspective of being "malicious", which takes into account such failures of LED transmitters, the system model in this section becomes valid. Namely, based on some prior knowledge (such as the LED brand and type, and previous operating experience), the probability of failure can be determined for each LED transmitter, and the model in (2) can be applied. In this case, it is reasonable to model that each LED transmitter can fail (i.e., become "malicious") independently of the others. (ii) Consider a hijacking attack in which the malicious third party gets the control of the whole VLP network by accessing the VLP controller. In this case, the malicious third party can randomly select some of the LED transmitters and modify their transmit powers in order not to be detected easily. Hence, the assumption of malicious LED transmitters in this section becomes valid in such a scenario, as well. (iii) Please also see Sections VII and VIII for extensions of the system model.

III. Position Estimation in the Presence of Malicious LED Transmitters

The aim of the VLC receiver is to estimate its location $\boldsymbol{l}_{\rm R}$ based on the power measurements in (1). Let $\boldsymbol{P}_{\rm R}$ represent a vector consisting of the power measurements; i.e., $\boldsymbol{P}_{\rm R} = [P_{{\rm R},1}\cdots P_{{\rm R},N_{\rm L}}]^T$. Also, let $\boldsymbol{P}_{\rm M}$ denote the vector of unknown transmit powers in (2); that is, $\boldsymbol{P}_{\rm M} = [P_{{\rm M},1}\cdots P_{{\rm M},N_{\rm L}}]^T$. In practice, upper and lower limits can be imposed on the elements of $\boldsymbol{P}_{\rm M}$ considering the specifications of the LEDs. Hence, it is assumed that $\boldsymbol{P}_{\rm M} \in \mathcal{P}$, where $\mathcal{P} = [P_{\min,1}, P_{\max,1}] \times \cdots \times [P_{\min,N_{\rm L}}, P_{\max,N_{\rm L}}]$. Similarly, let $\boldsymbol{l}_{\rm R} \in \mathcal{L}$, where $\mathcal{L}$ denotes the possible locations of the VLC receiver; e.g., all possible locations in a room or factory. It is assumed that there exists no prior statistical information about $\boldsymbol{P}_{\rm M}$ or $\boldsymbol{l}_{\rm R}$.

The location of the VLC receiver can be estimated via the ML estimator [44], which is stated as

$$\left(\widehat{\boldsymbol{l}}_{\rm R}, \widehat{\boldsymbol{P}}_{\rm M}\right) = \mathop{\arg\max}_{\boldsymbol{l}_{\rm R}\in\mathcal{L}, \boldsymbol{P}_{\rm M}\in\mathcal{P}} p(\boldsymbol{P}_{\rm R}\,|\,\boldsymbol{l}_{\rm R}, \boldsymbol{P}_{\rm M}) \tag{4}$$

In (4), $p(\boldsymbol{P}_{\rm R}\,|\,\boldsymbol{l}_{\rm R}, \boldsymbol{P}_{\rm M})$ denotes the likelihood function, which can be calculated from (1) and (2) as follows:

$$\begin{aligned} p(\boldsymbol{P}_{\rm R}\,|\,\boldsymbol{l}_{\rm R}, \boldsymbol{P}_{\rm M}) = \prod_{i=1}^{N_{\rm L}}\Bigg(&\frac{\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{{\rm R},i}-P_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \\ &+ \frac{1-\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}}\Bigg) \end{aligned} \tag{5}$$

From (4) and (5), it can be shown, after some manipulation, that the ML estimator for the location of the VLC receiver becomes

$$\begin{aligned} \widehat{\boldsymbol{l}}_{\rm R} = \mathop{\arg\max}_{\boldsymbol{l}_{\rm R}\in\mathcal{L}} \prod_{i=1}^{N_{\rm L}}\Bigg(&\frac{\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{{\rm R},i}-\widehat{P}_{{\rm M},i}(\boldsymbol{l}_{\rm R})R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \\ &+ \frac{1-\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}}\Bigg) \end{aligned} \tag{6}$$

where $\widehat{P}_{{\rm M},i}(\boldsymbol{l}_{\rm R})$ in (6) is given by

$$\widehat{P}_{{\rm M},i}(\boldsymbol{l}_{\rm R}) = \begin{cases} P_{\min,i}, & \text{if } \frac{P_{{\rm R},i}}{R_p h_i(\boldsymbol{l}_{\rm R})} \le P_{\min,i} \\ P_{\max,i}, & \text{if } \frac{P_{{\rm R},i}}{R_p h_i(\boldsymbol{l}_{\rm R})} \ge P_{\max,i} \\ \frac{P_{{\rm R},i}}{R_p h_i(\boldsymbol{l}_{\rm R})}, & \text{otherwise} \end{cases} \tag{7}$$

It is noted that the maximizer of the likelihood function in (5) over $P_{{\rm M},i}$ is obtained for any given value of $\boldsymbol{l}_{\rm R}$ as in (7), which leads to a significant reduction in computational complexity. Namely, the original formulation of the ML estimator in (4), which requires optimization over an $(N_{\rm L}+3)$-dimensional space is reduced to a three-dimensional search in (6).

IV. Position Estimation in the Presence of Malicious LED Transmitters and Training Measurements

In this section, we suppose that power measurements can be taken at known locations in a given environment beforehand for training purposes. Based on those measurements, information related to maliciousness of each LED transmitter can be collected, which can then be used for the location estimation of the VLC receiver.

The power measurements at N_{V} known locations, denoted by $\boldsymbol{l}_{\mathrm{R}}^{(1)}, \ldots, \boldsymbol{l}_{\mathrm{R}}^{(N_{\mathrm{V}})}$, can be expressed as follows:

$$P_{\mathrm{R},i}^{(j)} = R_p\, P_{\mathrm{T},i}^{(j)}\, h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) + \eta_i^{(j)} \tag{8}$$

for $i = 1, \ldots, N_{\mathrm{L}}$ and $j = 1, \ldots, N_{\mathrm{V}}$, where $P_{\mathrm{R},i}^{(j)}$ is the power measurement at location $\boldsymbol{l}_{\mathrm{R}}^{(j)}$ due to the signal emitted from the ith LED transmitter, $P_{\mathrm{T},i}^{(j)}$ denotes the transmit power of the ith LED transmitter during the measurement at location $\boldsymbol{l}_{\mathrm{R}}^{(j)}$, and $\eta_i^{(j)}$ is the noise component during the reception of the signal coming from the ith LED transmitter when the VLC receiver is at location $\boldsymbol{l}_{\mathrm{R}}^{(j)}$. The variance of $\eta_i^{(j)}$ is denoted by $\sigma_{i,j}^2$, and $\eta_i^{(j)}$'s are modeled as zero-mean Gaussian random variables that are independent for all i and j.

It is assumed that an LED transmitter is either malicious or honest during the training and estimation stages; i.e., its status does not change over the time interval of interest. In addition, two scenarios, named Scenario 1 and Scenario 2, are considered related to the transmit powers of the malicious LED transmitters.

Scenario 1: Each malicious LED transmitter employs a fixed unknown power level during all the measurements (i.e., during the training and estimation stages). Hence, parameter $P_{\mathrm{T},i}^{(j)}$ in (8) is modeled in Scenario 1 as

$$P_{\mathrm{T},i}^{(j)} = \begin{cases} P_{\mathrm{M},i}\,, & \text{with probability } \gamma_i \\ P_{\mathrm{H},i}\,, & \text{with probability } 1-\gamma_i \end{cases} \tag{9}$$

for $j \in \{1, \ldots, N_{\mathrm{V}}\}$.

Scenario 2: In this scenario, a malicious LED transmitter is modeled to change its transmit power frequently such that its transmit power can vary for each measurement. Then, $P_{\mathrm{T},i}^{(j)}$ in (8) is modeled as

$$P_{\mathrm{T},i}^{(j)} = \begin{cases} P_{\mathrm{M},i}^{(j)}\,, & \text{with probability } \gamma_i \\ P_{\mathrm{H},i}\,, & \text{with probability } 1-\gamma_i \end{cases} \tag{10}$$

for $j \in \{1, \ldots, N_{\mathrm{V}}\}$.

Based on the power measurements in (8), the aim is to make a decision for each LED transmitter about its status (malicious or honest), and to then perform localization based on a given power measurement vector $\boldsymbol{P}_{\mathrm{R}}$ (see (1)) by utilizing those decisions. The preceding two scenarios are investigated in the following.

A. Detection and Estimation in Scenario 1

In Scenario 1, the following binary hypothesis-testing problem can be formulated for the ith LED transmitter based on the measurements in (8):

$$\begin{aligned} \mathcal{H}_i \;&:\; P_{\mathrm{R},i}^{(j)} = R_p\, P_{\mathrm{H},i}\, h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) + \eta_i^{(j)},\ j = 1, \ldots, N_{\mathrm{V}} \\ \mathcal{M}_i \;&:\; P_{\mathrm{R},i}^{(j)} = R_p\, P_{\mathrm{M},i}\, h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) + \eta_i^{(j)},\ j = 1, \ldots, N_{\mathrm{V}} \end{aligned} \tag{11}$$

where $\mathcal{H}_i$ and $\mathcal{M}_i$ denote the hypotheses that the ith LED transmitter is honest and malicious, respectively.

As $P_{\mathrm{M},i}$'s are unknown, the hypothesis $\mathcal{M}_i$ is a composite hypothesis and the generalized likelihood ratio test (GLRT) is a well-suited approach for this problem due to the absence of prior distributions of $P_{\mathrm{M},i}$'s [44]. The GLRT for the problem in (11) can be stated as

$$\frac{\displaystyle\max_{P_{\mathrm{M},i}\in[P_{\min,i},P_{\max,i}]} \prod_{j=1}^{N_{\mathrm{V}}} \frac{e^{-\frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{M},i} h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}}{\sqrt{2\pi}\sigma_{i,j}}}{\displaystyle\prod_{j=1}^{N_{\mathrm{V}}} \frac{1}{\sqrt{2\pi}\sigma_{i,j}} e^{-\frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{H},i} h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \tau_i \tag{12}$$

where τ_i denotes the threshold, which can be chosen according to the tradeoff between the conditional probabilities of error [44]. In particular, since the probability distribution under $\mathcal{H}_i$ is completely known, the probability of deciding for $\mathcal{M}_i$ when $\mathcal{H}_i$ is true, i.e., the false alarm probability, can be fixed to a suitable value for setting the threshold.[1] (The effects of threshold selection on localization performance are investigated in Section VI.) The maximization problem in the numerator of (12) yields the following maximizer:

$$\widehat{P}_{\mathrm{M},i} = \begin{cases} P_{\min,i}, & \text{if } g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big) \le P_{\min,i} \\ P_{\max,i}, & \text{if } g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big) \ge P_{\max,i} \\ g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big), & \text{otherwise} \end{cases} \tag{13}$$

where

$$g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big) \triangleq \frac{\sum_{j=1}^{N_{\mathrm{V}}} P_{\mathrm{R},i}^{(j)} h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)/\sigma_{i,j}^2}{R_p \sum_{j=1}^{N_{\mathrm{V}}} \big(h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big)^2/\sigma_{i,j}^2} \tag{14}$$

Then, the GLRT in (12) can be simplified, after some manipulation, as follows:

$$\begin{aligned} &R_p\big(\widehat{P}_{\mathrm{M},i} - P_{\mathrm{H},i}\big) \sum_{j=1}^{N_{\mathrm{V}}} \frac{P_{\mathrm{R},i}^{(j)} h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)}{\sigma_{i,j}^2} \\ &+ 0.5 R_p^2 \Big(P_{\mathrm{H},i}^2 - \big(\widehat{P}_{\mathrm{M},i}\big)^2\Big) \sum_{j=1}^{N_{\mathrm{V}}} \frac{\big(h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big)^2}{\sigma_{i,j}^2} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \log(\tau_i) \end{aligned} \tag{15}$$

where $\widehat{P}_{\mathrm{M},i}$ is given by (13).

Let $\widehat{D}_i$ denote the decision of the GLRT in (15), i.e., the decision for the ith LED transmitter, where $i \in \{1, \ldots, N_{\mathrm{L}}\}$. When the power measurements $\boldsymbol{P}_{\mathrm{R}}$ are taken as in (1) related to a VLC receiver at an unknown location $\boldsymbol{l}_{\mathrm{R}}$, the problem becomes the estimation of $\boldsymbol{l}_{\mathrm{R}}$ based on $\boldsymbol{P}_{\mathrm{R}}$ and the decisions $\widehat{D}_1, \ldots, \widehat{D}_{N_{\mathrm{L}}}$. In Scenario 1, two approaches are considered as described in the following:

1) Algorithm 1-(a): In this algorithm, the decisions of the GLRTs in (15) and the power estimates in (13) are assumed to be perfect, and the probability distribution of $\boldsymbol{P}_{\mathrm{R}}$ is determined accordingly. In particular, let $\widehat{\mathcal{H}}$ and $\widehat{\mathcal{M}}$ denote the sets of honest and malicious LED transmitters according to the decision of the GLRTs in (15); that is,

$$\widehat{\mathcal{H}} = \{i \in \{1, \ldots, N_{\mathrm{L}}\} \mid \widehat{D}_i = \mathcal{H}_i\} \tag{16}$$

$$\widehat{\mathcal{M}} = \{i \in \{1, \ldots, N_{\mathrm{L}}\} \mid \widehat{D}_i = \mathcal{M}_i\} \tag{17}$$

[1] In particular, the threshold can be set via Monte-Carlo trials for a given false alarm probability by generating a sufficient number of received power measurements according to the $\mathcal{H}_i$ hypothesis (see (11)).

Then, the likelihood function from this perspective can be expressed as

$$p(\boldsymbol{P}_{\rm R}\,|\,\boldsymbol{l}_{\rm R}) = \prod_{i\in\widehat{\mathcal{H}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \times \prod_{i\in\widehat{\mathcal{M}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-\widehat{P}_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \tag{18}$$

and the resulting ML estimator can be derived as

$$\widehat{\boldsymbol{l}}_{\rm R} = \mathop{\arg\min}_{\boldsymbol{l}_{\rm R}\in\mathcal{L}} \sum_{i\in\widehat{\mathcal{H}}} \frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2} + \sum_{i\in\widehat{\mathcal{M}}} \frac{(P_{{\rm R},i}-\widehat{P}_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2} \tag{19}$$

where $\widehat{P}_{{\rm M},i}$ is as in (13) for $i\in\widehat{\mathcal{M}}$.

2) Algorithm 1-(b): In this algorithm, the estimates in (13) are still assumed to be perfect but possible errors in the decisions of the GLRTs in (15) are taken into consideration. Specifically, the probability that the ith LED transmitter is malicious is calculated as follows:

$$\widehat{\gamma}_i = {\rm P}(\mathcal{M}_i\,|\,\widehat{D}_i) = \frac{\gamma_i {\rm P}(\widehat{D}_i\,|\,\mathcal{M}_i)}{\gamma_i {\rm P}(\widehat{D}_i\,|\,\mathcal{M}_i) + (1-\gamma_i){\rm P}(\widehat{D}_i\,|\,\mathcal{H}_i)} \tag{20}$$

where $\gamma_i = {\rm P}(\mathcal{M}_i)$ as defined before. In other words, in Algorithm 1-(b), the probabilities are updated according to the decisions produced by the GLRTs in the training stage. Hence, γ_i and $\widehat{\gamma}_i$ can be regarded, respectively, as the prior and posterior probabilities that the ith LED is malicious. Accordingly, the ML estimator can be obtained as follows:

$$\widehat{\boldsymbol{l}}_{\rm R} = \mathop{\arg\max}_{\boldsymbol{l}_{\rm R}\in\mathcal{L}} \prod_{i=1}^{N_{\rm L}} \left(\frac{\widehat{\gamma}_i}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-\widehat{P}_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} + \frac{1-\widehat{\gamma}_i}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \right) \tag{21}$$

where $\widehat{\gamma}_i$ is given by (20) and $\widehat{P}_{{\rm M},i}$ is as in (13). It should be noted that ${\rm P}(\widehat{D}_i\,|\,\mathcal{M}_i)$ and ${\rm P}(\widehat{D}_i\,|\,\mathcal{H}_i)$ can be calculated for the GLRT in (15) based on analytical approaches or simply via Monte-Carlo trials.

B. Detection and Estimation in Scenario 2

In this scenario, the hypothesis-testing problem for the ith LED transmitter can be stated as

$$\begin{aligned} \mathcal{H}_i &: P_{{\rm R},i}^{(j)} = R_p\, P_{{\rm H},i}\, h_i\big(\boldsymbol{l}_{\rm R}^{(j)}\big) + \eta_i^{(j)},\ j=1,\dots,N_{\rm V} \\ \mathcal{M}_i &: P_{{\rm R},i}^{(j)} = R_p\, P_{{\rm M},i}^{(j)}\, h_i\big(\boldsymbol{l}_{\rm R}^{(j)}\big) + \eta_i^{(j)},\ j=1,\dots,N_{\rm V} \end{aligned} \tag{22}$$

Then, the GLRT is given by

$$\frac{\displaystyle\max_{\{P_{{\rm M},i}^{(j)}\}_{j=1}^{N_{\rm V}}} \prod_{j=1}^{N_{\rm V}} \frac{1}{\sqrt{2\pi}\sigma_{i,j}} e^{-\frac{\left(P_{{\rm R},i}^{(j)}-R_p P_{{\rm M},i}^{(j)} h_i\left(\boldsymbol{l}_{\rm R}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}}{\displaystyle\prod_{j=1}^{N_{\rm V}} \frac{1}{\sqrt{2\pi}\sigma_{i,j}} e^{-\frac{\left(P_{{\rm R},i}^{(j)}-R_p P_{{\rm H},i} h_i\left(\boldsymbol{l}_{\rm R}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \kappa_i \tag{23}$$

where κ_i denotes the threshold. The maximization problem in the numerator of (23) can be solved in closed form, which leads to the following simplified form of the GLRT after some manipulation:

$$\sum_{j=1}^{N_{\rm V}} \frac{1}{\sigma_{i,j}^2} \Big(R_p P_{{\rm R},i}^{(j)} h_i\big(\boldsymbol{l}_{\rm R}^{(j)}\big)\big(\widehat{P}_{{\rm M},i}^{(j)} - P_{{\rm H},i}\big) + 0.5 R_p^2 \big(h_i\big(\boldsymbol{l}_{\rm R}^{(j)}\big)\big)^2 \Big(P_{{\rm H},i}^2 - \big(\widehat{P}_{{\rm M},i}^{(j)}\big)^2\Big)\Big) \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \log(\kappa_i) \tag{24}$$

where

$$\widehat{P}_{{\rm M},i}^{(j)} = \begin{cases} P_{\min,i}\,, & \text{if } \dfrac{P_{{\rm R},i}^{(j)}}{R_p h_i\left(\boldsymbol{l}_{\rm R}^{(j)}\right)} \le P_{\min,i} \\ P_{\max,i}\,, & \text{if } \dfrac{P_{{\rm R},i}^{(j)}}{R_p h_i\left(\boldsymbol{l}_{\rm R}^{(j)}\right)} \ge P_{\max,i} \\ \dfrac{P_{{\rm R},i}^{(j)}}{R_p h_i\left(\boldsymbol{l}_{\rm R}^{(j)}\right)}\,, & \text{otherwise} \end{cases} \tag{25}$$

Let $\widehat{D}_i$ denote the decision of the GLRT in (24) for $i\in\{1,\dots,N_{\rm L}\}$. When the power measurements $\boldsymbol{P}_{\rm R}$ are taken as in (1) related to a VLC receiver at an unknown location $\boldsymbol{l}_{\rm R}$, the estimation of $\boldsymbol{l}_{\rm R}$ can be performed via the following algorithms in Scenario 2:

1) Algorithm 2-(a): In this algorithm, the decisions of the GLRTs in (24) are assumed to be correct and the likelihood function is stated as

$$p(\boldsymbol{P}_{\rm R}\,|\,\boldsymbol{l}_{\rm R},\boldsymbol{P}_{\rm M}) = \prod_{i\in\widehat{\mathcal{H}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \times \prod_{i\in\widehat{\mathcal{M}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-P_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \tag{26}$$

where $\widehat{\mathcal{H}}$ and $\widehat{\mathcal{M}}$ are as defined in (16) and (17), respectively, for the GLRTs in (24). Then, the corresponding ML estimator is derived as

$$\widehat{\boldsymbol{l}}_{\rm R} = \mathop{\arg\min}_{\boldsymbol{l}_{\rm R}} \sum_{i\in\widehat{\mathcal{H}}} \frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2} + \sum_{i\in\widehat{\mathcal{M}}} \frac{(P_{{\rm R},i}-\widehat{P}_{{\rm M},i}(\boldsymbol{l}_{\rm R})R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2} \tag{27}$$

where $\widehat{P}_{{\rm M},i}(\boldsymbol{l}_{\rm R})$ is as in (7) for $i\in\widehat{\mathcal{M}}$.

2) Algorithm 2-(b): In this algorithm, possible errors in the decisions of the GLRTs in (24) are considered by updating the probabilities that the LED transmitters can be malicious as in (20). Then, the ML estimator is designed as in Section III by replacing γ_i's with $\widehat{\gamma}_i$'s. Consequently, Algorithm 2-(b) can be expressed as in (6) and (7) by replacing γ_i's in (6) with $\widehat{\gamma}_i$'s obtained from (20).

Remark 3: It is noted that the estimates obtained in the training stage for the power levels of the malicious LED transmitters in (25) are not employed during the estimation stage since the power levels of the malicious LED transmitters vary in Scenario 2 (i.e., they become different in the estimation stage).

Remark 4: It is noted that Algorithm 1-(a) and Algorithm 2-(a) can be implemented without using the probabilities that the

LED transmitters can be malicious. However, the knowledge of these probabilities is required for Algorithm 1-(b) and Algorithm 2-(b). In practice, the knowledge of the probabilities that the LED transmitters are malicious can be obtained in various ways: (i) For the case in which an LED transmitter becomes "malicious" due a failure in the LED chip (see Remark 2), the probability that an LED can fail can be learned based on some prior knowledge depending on the LED brand and type or based on previous operating experience. (ii) For the case in which an LED transmitter becomes malicious due to hijacking, the probability of such an event can be estimated based on the history of VLP networks operating in similar environments/conditions.

C. Alternative Detection Approach for Scenario 1

In Section IV-A, the GLRT is obtained as in (15) and its threshold is set according to the tradeoff between the conditional probabilities of error, namely, $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{M}_i)$ and $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{H}_i)$. As an alternative approach, the uniformly most powerful (UMP) test can be derived in Scenario 1 if there exists prior information that a malicious LED transmitter does not increase the power level with respect to the power level of an honest LED transmitter; that is, if the following condition is satisfied:

$$P_{\mathrm{M},i} \leq P_{\mathrm{H},i}\,,\ \forall i \tag{28}$$

Under this condition, the likelihood ratio test for the hypothesis-testing problem in (11) can be expressed as

$$\frac{\exp\left\{\sum_{j=1}^{N_{\mathrm{V}}} \frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{H},i} h_i(\boldsymbol{l}_{\mathrm{R}}^{(j)})\right)^2}{2\sigma_{ij}^2}\right\}}{\exp\left\{\sum_{j=1}^{N_{\mathrm{V}}} \frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{M},i} h_i(\boldsymbol{l}_{\mathrm{R}}^{(j)})\right)^2}{2\sigma_{ij}^2}\right\}} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \eta_i \tag{29}$$

where η_i denotes the threshold. Taking the natural logarithm of both sides leads to

$$\begin{aligned}&\sum_{j=1}^{N_{\mathrm{V}}} \frac{R_p h_i(\boldsymbol{l}_{\mathrm{R}}^{(j)}) P_{\mathrm{R},i}^{(j)} (P_{\mathrm{M},i} - P_{\mathrm{H},i})}{\sigma_i^2} \\ &+ \sum_{j=1}^{N_{\mathrm{V}}} \frac{R_p^2 h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)}) \left(P_{\mathrm{H},i}^2 - P_{\mathrm{M},i}^2\right)}{2\sigma_i^2} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \log \eta_i\end{aligned} \tag{30}$$

Based on the condition in (28), the expression in (30) can be simplified as

$$\sum_{j=1}^{N_{\mathrm{V}}} \frac{P_{\mathrm{R},i}^{(j)} h_i(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2} \underset{\mathcal{M}_i}{\overset{\mathcal{H}_i}{\gtrless}} \tilde{\eta}_i \tag{31}$$

where $\tilde{\eta}_i$ is defined as $\tilde{\eta}_i \triangleq \big(\log \eta_i - \sum_{j=1}^{N_{\mathrm{V}}} R_p^2 h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)})(P_{\mathrm{H},i}^2 - P_{\mathrm{M},i}^2)/(2\sigma_i^2)\big)/(R_p(P_{\mathrm{M},i} - P_{\mathrm{H},i}))$. For the test in (31), the false alarm probability can be derived analytically as follows. Under hypothesis $\mathcal{H}_i$ in Scenario 1 (see (11)), the received power $P_{\mathrm{R},i}^{(j)}$ follows a Gaussian distribution with mean $R_p P_{\mathrm{H},i} h_i(\boldsymbol{l}_{\mathrm{R}}^{(j)})$ and variance σ_{ij}^2; i.e.,

$$P_{\mathrm{R},i}^{(j)} \sim \mathcal{N}\big(R_p P_{\mathrm{H},i} h_i(\boldsymbol{l}_{\mathrm{R}}^{(j)}), \sigma_{ij}^2\big) \tag{32}$$

Since $P_{\mathrm{R},i}^{(j)}$'s are independent for different j's, we get

$$\sum_{j=1}^{N_{\mathrm{V}}} \frac{P_{\mathrm{R},i}^{(j)} h_i(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2} \sim \mathcal{N}\left(\sum_{j=1}^{N_{\mathrm{V}}} \frac{R_p P_{\mathrm{H},i} h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2}, \sum_{j=1}^{N_{\mathrm{V}}} \frac{h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2}\right) \tag{33}$$

Accordingly, setting the false alarm probability to a given level α leads to

$$1 - Q\left(\frac{\tilde{\eta}_i - \sum_{j=1}^{N_{\mathrm{V}}} \frac{R_p P_{\mathrm{H},i} h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2}}{\sqrt{\sum_{j=1}^{N_{\mathrm{V}}} \frac{h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2}}}\right) = \alpha \tag{34}$$

Then, solving for $\tilde{\eta}_i$ yields the following threshold:

$$\tilde{\eta}_i = \sqrt{\sum_{j=1}^{N_{\mathrm{V}}} \frac{h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2}}\, Q^{-1}(1-\alpha) + \sum_{j=1}^{N_{\mathrm{V}}} \frac{R_p P_{\mathrm{H},i} h_i^2(\boldsymbol{l}_{\mathrm{R}}^{(j)})}{\sigma_{ij}^2} \tag{35}$$

Since the test in (31) with the threshold specified by (35) is a likelihood ratio test (as it is equivalent to (29)) and does change with respect to the unknown parameter $P_{\mathrm{M},i}$, it is a UMP test for the problem in (11) [44]. Hence, when the assumption in (28) holds, the UMP test exists for Scenario 1 and can be obtained as described in this section (which can be used instead of the GLRT in (15)). It should be noted that if the condition in (28) is reversed, i.e., if $P_{\mathrm{M},i} > P_{\mathrm{H},i}$, $\forall i$, a UMP test can again be derived based on a similar argument. However, it is more likely for a malicious third party to reduce the transmit powers of the LED transmitters to degrade the positioning accuracy.

V. CRLB Derivations

In this section, CRLB expressions are derived for three different cases to establish benchmarks for performance of the proposed algorithms in the absence and presence of training measurements. In the first case, it is assumed that the transmit powers of all the LEDs, i.e., $\{P_{\mathrm{T},i}\}_{i=1}^{N_{\mathrm{L}}}$, are perfectly known. This bound applies to Scenario 1, in which the transmit power of each malicious LED transmitter is fixed and can be estimated via training measurements. In the second case, it is assumed that the transmit power of malicious LED transmitters are unknown but their indices are known. This bound corresponds to Scenario 2, in which there exist training measurements and malicious LED transmitters modify their transmit powers for each measurement. In the third case, the CRLB is derived for the scenario without training measurements, which corresponds to the setting considered in Section III. Overall, via three different CRLB derivations, we take into account various levels of knowledge related to the transmit powers of the malicious LED transmitters and the indices of malicious LEDs.

A. CRLB for Scenario 1 (Knowledge of Transmit Powers)

In this case, the transmit powers of all the LEDs, i.e., $\{P_{\mathrm{T},i}\}_{i=1}^{N_{\mathrm{L}}}$, are perfectly known. Therefore, the vector of unknown parameters consists only of the PD location, i.e.,

$\boldsymbol{l}_\mathrm{R}$. Thus, the likelihood function for $\boldsymbol{l}_\mathrm{R}$ based on the measurements in (1) can be expressed as

$$p(\boldsymbol{P}_\mathrm{R}|\boldsymbol{l}_\mathrm{R}) = \left(\prod_{i=1}^{N_\mathrm{L}} \frac{1}{\sqrt{2\pi}\sigma_i}\right) e^{-\sum_{i=1}^{N_\mathrm{L}} \frac{(P_{\mathrm{R},i}-R_p P_{\mathrm{T},i} h_i(\boldsymbol{l}_\mathrm{R}))^2}{2\sigma_i^2}} \tag{36}$$

Then, the Fisher information matrix (FIM) is given by

$$\boldsymbol{J}(\boldsymbol{l}_\mathrm{R}) = \mathbb{E}\{(\nabla_{\boldsymbol{l}_\mathrm{R}} \log p(\boldsymbol{P}_\mathrm{R}|\boldsymbol{l}_\mathrm{R}))(\nabla_{\boldsymbol{l}_\mathrm{R}} \log p(\boldsymbol{P}_\mathrm{R}|\boldsymbol{l}_\mathrm{R}))^T\} \tag{37}$$

and the CRLB is expressed as [44]

$$\mathbb{E}\big\{\big\|\widehat{\boldsymbol{l}}_\mathrm{R} - \boldsymbol{l}_\mathrm{R}\big\|^2\big\} \geq \mathrm{trace}\big\{\boldsymbol{J}(\boldsymbol{l}_\mathrm{R})^{-1}\big\} \triangleq CRLB \tag{38}$$

After some manipulation, the elements of the FIM in (37) can be calculated from (36) as follows:

$$[\boldsymbol{J}(\boldsymbol{l}_\mathrm{R})]_{p,q} = R_P^2 \sum_{i=1}^{N_\mathrm{L}} \frac{P_{\mathrm{T},i}^2}{\sigma_i^2} \frac{\partial h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(p)} \frac{\partial h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(q)} \tag{39}$$

where $p, q \in \{1, 2, 3\}$ and $\boldsymbol{l}_\mathrm{R}(p)$ denotes the pth element of $\boldsymbol{l}_\mathrm{R}$. In addition, based on (3), the partial derivatives of $h_i(\boldsymbol{l}_\mathrm{R})$ with respect to $\boldsymbol{l}_\mathrm{R}(p)$ can be expressed as

$$\begin{aligned}\frac{\partial h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(p)} = \frac{(m_i+1)A_\mathrm{R}}{2\pi} \Bigg(& \frac{\boldsymbol{g}_{1\mathrm{p}}^i(\boldsymbol{l}_\mathrm{R})\boldsymbol{g}_2^i(\boldsymbol{l}_\mathrm{R}) + \boldsymbol{g}_1^i(\boldsymbol{l}_\mathrm{R})\boldsymbol{g}_{2\mathrm{p}}^i(\boldsymbol{l}_\mathrm{R})}{\boldsymbol{g}_3^i(\boldsymbol{l}_\mathrm{R})} \\ & - \frac{\boldsymbol{g}_1^i(\boldsymbol{l}_\mathrm{R})\boldsymbol{g}_2^i(\boldsymbol{l}_\mathrm{R})\boldsymbol{g}_{3\mathrm{p}}^i(\boldsymbol{l}_\mathrm{R})}{{\boldsymbol{g}_3^i}^2(\boldsymbol{l}_\mathrm{R})}\Bigg)\end{aligned} \tag{40}$$

where

$$\boldsymbol{g}_1^i(\boldsymbol{l}_\mathrm{R}) = \big[(\boldsymbol{l}_\mathrm{R} - \boldsymbol{l}_\mathrm{T}^i)^T \boldsymbol{n}_\mathrm{T}^i\big]^{m_i} \tag{41}$$

$$\boldsymbol{g}_2^i(\boldsymbol{l}_\mathrm{R}) = (\boldsymbol{l}_\mathrm{T}^i - \boldsymbol{l}_\mathrm{R})^T \boldsymbol{n}_\mathrm{R} \tag{42}$$

$$\boldsymbol{g}_3^i(\boldsymbol{l}_\mathrm{R}) = \big\|\boldsymbol{l}_\mathrm{R} - \boldsymbol{l}_\mathrm{T}^i\big\|^{m_i+3} \tag{43}$$

$$\boldsymbol{g}_{1\mathrm{p}}^i(\boldsymbol{l}_\mathrm{R}) = \frac{\partial \boldsymbol{g}_1^i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(p)} = m_i \big[(\boldsymbol{l}_\mathrm{R} - \boldsymbol{l}_\mathrm{T}^i)^T \boldsymbol{n}_\mathrm{T}^i\big]^{m_i-1} \boldsymbol{n}_\mathrm{T}^i(p) \tag{44}$$

$$\boldsymbol{g}_{2\mathrm{p}}^i(\boldsymbol{l}_\mathrm{R}) = \frac{\partial \boldsymbol{g}_2^i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(p)} = -\boldsymbol{n}_\mathrm{R}(p) \tag{45}$$

$$\begin{aligned}\boldsymbol{g}_{3\mathrm{p}}^i(\boldsymbol{l}_\mathrm{R}) = \frac{\partial \boldsymbol{g}_3^i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(p)} &= (m_i+3)\big\|\boldsymbol{l}_\mathrm{R} - \boldsymbol{l}_\mathrm{T}^i\big\|^{m_i+1} \\ &\quad \times \big[(\boldsymbol{l}_\mathrm{R}(p) - \boldsymbol{l}_\mathrm{T}^i(p))\big]\end{aligned} \tag{46}$$

Thus, the CRLB can be obtained from (38)–(46), yielding a lower bound on mean-squared errors (MSEs) of unbiased estimators for $\boldsymbol{l}_\mathrm{R}$ when the transmit powers of the LEDs are known. Since the malicious LEDs employ fixed transmit powers that can be learned via training measurements in Scenario 1, the CRLB expression in this section applies to Scenario 1; hence, it is referred to as "CRLB - Scen. 1" in Section VI.

B. CRLB for Scenario 2 (Knowledge of Indices of Malicious LEDs)

In this case, it is assumed that the transmit powers of the malicious LEDs are unknown but their indices are known. The set of indices of the malicious LEDs is expressed as

$$\mathcal{M} = \{i \in \{1, \ldots, N_\mathrm{L}\} \,|\, i\text{th LED is malicious}\} \tag{47}$$

and the number of elements in $\mathcal{M}$ is denoted by M_L. Then, the vector of unknown parameters is defined as

$$\boldsymbol{\Theta} = \big[\boldsymbol{l}_\mathrm{R}^T \ \boldsymbol{P}_\mathrm{M}^T\big]^T \tag{48}$$

where $\boldsymbol{P}_\mathrm{M}$ is the vector consisting of the transmit powers of the malicious LEDs. Accordingly, the likelihood function for $\boldsymbol{\Theta}$ based on the measurements in (1) can be expressed as

$$p(\boldsymbol{P}_\mathrm{R}|\boldsymbol{\Theta}) = \left(\prod_{i=1}^{N_\mathrm{L}} \frac{1}{\sqrt{2\pi}\sigma_i}\right) e^{-\sum_{i=1}^{N_\mathrm{L}} \frac{(P_{\mathrm{R},i}-R_p P_{\mathrm{T},i} h_i(\boldsymbol{l}_\mathrm{R}))^2}{2\sigma_i^2}} \tag{49}$$

and the FIM is given by

$$\boldsymbol{J}(\boldsymbol{\Theta}) = \mathbb{E}\{(\nabla_{\boldsymbol{\Theta}} \log p(\boldsymbol{P}_\mathrm{R}|\boldsymbol{\Theta}))(\nabla_{\boldsymbol{\Theta}} \log p(\boldsymbol{P}_\mathrm{R}|\boldsymbol{\Theta}))^T\} \tag{50}$$

Based on the FIM, the bound on the estimation error for the location $\boldsymbol{l}_\mathrm{R}$ of the VLC receiver can be specified as

$$\mathbb{E}\big\{\big\|\widehat{\boldsymbol{l}}_\mathrm{R} - \boldsymbol{l}_\mathrm{R}\big\|^2\big\} \geq \mathrm{trace}\big\{\boldsymbol{J}(\boldsymbol{\Theta})^{-1}_{1:3,1:3}\big\} \triangleq CRLB_{\boldsymbol{l}_\mathrm{R}} \tag{51}$$

where $\widehat{\boldsymbol{l}}_\mathrm{R}$ denotes any unbiased estimator of $\boldsymbol{l}_\mathrm{R}$. Likewise, the bound on the estimation error for the transmit powers of the malicious LEDs can be stated as

$$\mathbb{E}\big\{\big\|\widehat{\boldsymbol{P}}_\mathrm{M} - \boldsymbol{P}_\mathrm{M}\big\|^2\big\} \geq \mathrm{trace}\big\{\boldsymbol{J}(\boldsymbol{\Theta})^{-1}_{4:M_L+3,4:M_L+3}\big\} \triangleq CRLB_{\boldsymbol{P}_\mathrm{M}} \tag{52}$$

where $\widehat{\boldsymbol{P}}_\mathrm{M}$ represents any unbiased estimator of $\boldsymbol{P}_\mathrm{M}$. After some manipulation, the elements of the FIM in (50) can be calculated from (49) as

$$[\boldsymbol{J}(\boldsymbol{\Theta})]_{p,q} = R_P^2 \sum_{i=1}^{N_\mathrm{L}} \frac{1}{\sigma_i^2} \frac{\partial P_{\mathrm{T},i} h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{\Theta}(p)} \frac{\partial P_{\mathrm{T},i} h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{\Theta}(q)} \tag{53}$$

where $p, q \in \{1, \ldots, M_L + 3\}$ and $\boldsymbol{\Theta}(p)$ denotes the pth element of $\boldsymbol{\Theta}$. As in Section V-A, for $p \in \{1, 2, 3\}$

$$\frac{\partial P_{\mathrm{T},i} h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{\Theta}(p)} = P_{\mathrm{T},i} \frac{\partial h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(p)} \tag{54}$$

where $\frac{\partial h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{l}_\mathrm{R}(p)}$ is as defined in (40), and for $p \in \{4, \ldots, M_L + 3\}$

$$\frac{\partial P_{\mathrm{T},i} h_i(\boldsymbol{l}_\mathrm{R})}{\partial \boldsymbol{\Theta}(p)} = h_i(\boldsymbol{l}_\mathrm{R}) \frac{\partial P_{\mathrm{T},i}}{\partial \boldsymbol{P}_\mathrm{M}(p-3)} \tag{55}$$

where

$$\frac{\partial P_{\mathrm{T},i}}{\partial \boldsymbol{P}_\mathrm{M}(p-3)} = \begin{cases} 1\,, & \text{if } i \in \mathcal{M} \text{ and } i = p-3 \\ 0\,, & \text{otherwise} \end{cases} \tag{56}$$

The CRLB expression specified by (51) and (54)–(56) provides a lower bound on position estimation in Scenario 2 since the indices of malicious LED transmitters can be learned via training measurements in that scenario. (However, the transmit powers of malicious LEDs cannot be learned since they change for each measurement in Scenario 2.) Therefore, it is referred to as "CRLB - Scen. 2" in Section VI.

C. CRLB without Training Measurements

In this case, neither the transmit powers nor the indices of the malicious LEDs are known. Therefore, the likelihood function in (5) is used to derive the CRLB. The natural logarithm of (5) can be expressed as

$$\log p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta}) = \sum_{i=1}^{N_{\rm L}} \log\left(\gamma_i E_M + (1-\gamma_i)E_H\right) \tag{57}$$

where $\boldsymbol{\Theta}$ is as defined in (48), and

$$E_M \triangleq \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-P_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \tag{58}$$

$$E_H \triangleq \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2}{2\sigma_i^2}} \tag{59}$$

Based on (57), the FIM is constructed as

$$\boldsymbol{J}(\boldsymbol{\Theta}) = \mathbb{E}\{(\nabla_{\boldsymbol{\Theta}} \log p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta}))(\nabla_{\boldsymbol{\Theta}} \log p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta}))^T\} \tag{60}$$

The partial derivatives in (60) can be expressed as follows:

$$\begin{aligned} &\frac{\partial \log p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta})}{\partial \boldsymbol{l}_{\rm R}(p)} \\ &= \sum_{i=1}^{N_{\rm L}} \frac{\gamma_i E_M (P_{{\rm R},i}-P_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))P_{{\rm M},i}R_p}{\sigma_i^2 p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta})} \frac{\partial h_i(\boldsymbol{l}_{\rm R})}{\partial \boldsymbol{l}_{\rm R}(p)} \\ &+ \sum_{i=1}^{N_{\rm L}} \frac{(1-\gamma_i) E_H (P_{{\rm R},i}-P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))P_{{\rm H},i}R_p}{\sigma_i^2 p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta})} \frac{\partial h_i(\boldsymbol{l}_{\rm R})}{\partial \boldsymbol{l}_{\rm R}(p)} \end{aligned} \tag{61}$$

$$\frac{\partial \log p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta})}{\partial \boldsymbol{P}_{\rm M}(p)} = \sum_{i=1}^{N_{\rm L}} \frac{\gamma_i E_M (P_{{\rm R},i}-P_{{\rm M},i}R_p h_i(\boldsymbol{l}_{\rm R}))R_p h_i(\boldsymbol{l}_{\rm R})}{\sigma_i^2 p(\boldsymbol{P}_{\rm R}|\boldsymbol{\Theta})} \tag{62}$$

The partial derivatives $\frac{\partial h_i(\boldsymbol{l}_{\rm R})}{\partial \boldsymbol{l}_{\rm R}(p)}$ are the same as in (40). As the expectation in (60) is hard to evaluate analytically, Monte Carlo integration methods can be used to compute the CRLB in a similar fashion to that in [45]. Namely, the FIM in (60) can be approximated as follows:

$$\boldsymbol{J}(\boldsymbol{\Theta}) \approx \frac{1}{N_{\rm MC}} \sum_{i=1}^{N_{\rm MC}} \left(\nabla_{\boldsymbol{\Theta}} \log p\big(\boldsymbol{P}_{\rm R}^{(i)}|\boldsymbol{\Theta}\big)\right)\left(\nabla_{\boldsymbol{\Theta}} \log p\big(\boldsymbol{P}_{\rm R}^{(i)}|\boldsymbol{\Theta}\big)\right)^T \tag{63}$$

where $N_{\rm MC}$ is the number of Monte-Carlo trials and $\boldsymbol{P}_{\rm R}^{(i)}$ is the realization of $\boldsymbol{P}_{\rm R}$ in the ith trial. In (63), $\nabla_{\boldsymbol{\Theta}} \log p\big(\boldsymbol{P}_{\rm R}^{(i)}|\boldsymbol{\Theta}\big)$ is evaluated based on the expressions in (61) and (62) for the given realization $\boldsymbol{P}_{\rm R}^{(i)}$. Hence, a semi-analytic evaluation approach is employed. Finally, the CRLB can be expressed as

$$\mathbb{E}\big\{\big\|\widehat{\boldsymbol{l}}_{\rm R} - \boldsymbol{l}_{\rm R}\big\|^2\big\} \geq {\rm trace}\big\{\boldsymbol{J}(\boldsymbol{\Theta})^{-1}_{1:3,1:3}\big\} \triangleq CRLB_{\boldsymbol{l}_{\rm R}} \tag{64}$$

This bound is referred to as "CRLB - No Training" in Section VI.

VI. Simulation Results

In this section, simulations are conducted to evaluate the performance of the proposed approaches. A room with dimensions $4 \times 4 \times 3$ meters (width, depth and height, respectively) is considered. The number of LED transmitters is taken as $N_{\rm L} = 9$ and they are placed at the following locations: $\{(-1,1,3),(0,1,3),(1,1,3),(-1,0,3),(0,0,3),(1,0,3),$ $(-1,-1,3),(0,-1,3),(1,-1,3)\}$ (all in meters) such that they cover the room in a symmetric manner, where $(0,0,0)$ corresponds to the center of the room floor. The orientation vectors, $\boldsymbol{n}_{\rm T}^i$'s, are taken as $[0,0,-1]^T$ $\forall i$ such that all the LEDs face downwards. Also, m_i's are set to 1 $\forall i$. Although the derivations in Section III and Section IV are generic for any three-dimensional setup, the VLC receiver is considered to be at a fixed height of 0.85 meters in the simulations (i.e., a two-dimensional localization scenario is considered [46]). Moreover, the orientation of the receiver is specified as $\boldsymbol{n}_{\rm R} = [0,0,1]^T$, i.e., it faces upwards, the area of the PD is taken as $A_{\rm R} = 1\,{\rm cm}^2$, and the responsivity of the PD is set to $R_p = 1$. Moreover, the noise variances are assumed to be the same, that is, $\sigma_i^2 = \sigma^2$ for $i = 1,\ldots,N_{\rm L}$.

Since the localization problem can be ill-posed when the number of honest LED transmitters is below 3, the probabilities that the LED transmitters can be malicious are set as follows:

$$\gamma_i = \begin{cases} 0, & \text{if } i = 1,6,7 \\ \gamma, & \text{otherwise} \end{cases} \tag{65}$$

Namely, in the simulations, it is guaranteed that there exist at least 3 honest LED transmitters for any given scenario. It should be noted that the indices of these 3 "always honest" LED transmitters is not known by the VLC receiver and that the other LED transmitters can also be honest with probability $(1-\gamma)$ independently of each other.

To investigate the performance of the proposed ML estimator in (6) (which is designed for the scenario without training measurements), the location of the VLC receiver is set to $\boldsymbol{l}_{\rm R} = [0.5\ 0.5\ 0.85]^T$ meters and various values of γ are considered. For each γ, 10^4 different sets of honest and malicious LED realizations are obtained according to (65), and the powers of the malicious LED transmitters, $P_{{\rm M},i}$'s, are generated as uniform random variables in the set $[1\,W, 3\,W]$, whereas the honest LED transmit power is set to $5\,W$. In addition, $P_{\min,i}$ is set to $1\,W$ and $P_{\max,i}$ is set to $10\,W$, which are the estimation parameters used in (7), (13), and (25).

In Fig. 1, the root-mean squared error (RMSE) performance of the proposed ML estimator in (6) is plotted versus γ for $\sigma^2 = 10^{-11}$. For comparison purposes, we also consider the case in which the VLC receiver is unaware of the security issue and assumes that all the LED transmitters are honest. In this case, the VLC receiver employs the model in (1) with $P_{{\rm T},i} = P_{{\rm H},i}$ for $i = 1,\ldots,N_{\rm L}$, which results in the following ML estimator: $\widehat{\boldsymbol{l}}_{\rm R} = \underset{\boldsymbol{l}_{\rm R}\in\mathcal{L}}{\arg\min} \sum_{i=1}^{N_{\rm L}} (P_{{\rm R},i} - P_{{\rm H},i}R_p h_i(\boldsymbol{l}_{\rm R}))^2/(2\sigma_i^2)$. This ML estimator is labeled as "ML – Unaware" in Fig. 1. As another way of comparison, the ML estimator in the presence of perfect knowledge of malicious LED transmitters is considered, which is given by (27) when $\widehat{\mathcal{H}}$ and $\widehat{\mathcal{M}}$ are equal

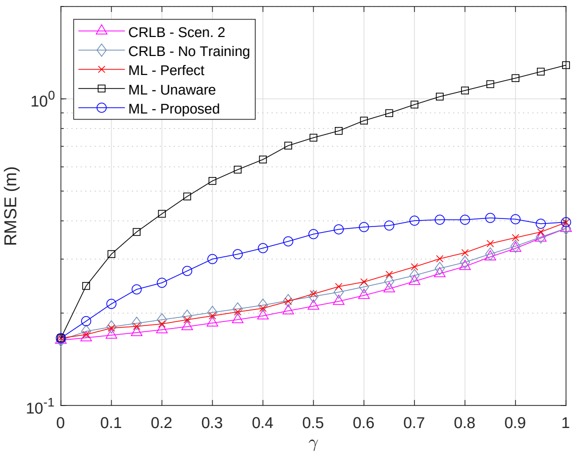


Fig. 1: RMSE versus γ for $\sigma^2 = 10^{-11}$.

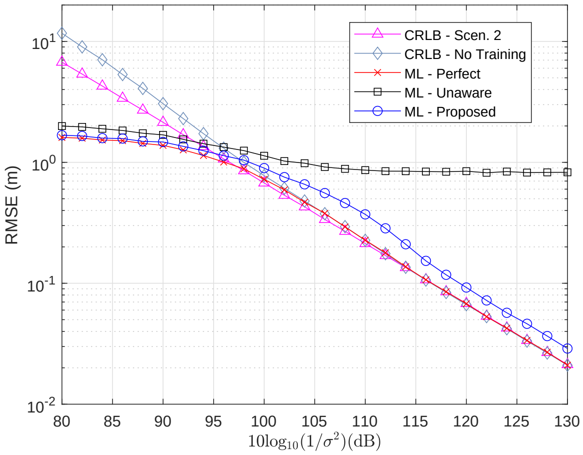


Fig. 2: RMSE versus $10\log_{10}(1/\sigma^2)$ for $\gamma = 0.5$.

to the correct sets of honest and malicious LED transmitters, respectively. This ML estimator is labeled as "ML – Perfect" in Fig. 1. The results in the figure show that the proposed estimator in (6) provides performance improvements (especially when γ is not small) over the estimator that assumes that all the LED transmitters are honest. Also, the estimator that perfectly knows which LED transmitters are malicious provides a performance lower bound, as expected. In addition, the estimators have higher RMSE values as γ increases due to the increased level of uncertainty about transmission powers. In Fig. 1, we also present the CRLB in the absence of training measurements ("CRLB - No Training") and the CRLB when the indices of malicious LED transmitters are known ("CRLB - Scen. 2"). The CRLB with no training measurements provides a lower bound on the performance of the proposed ML estimator. On the other hand, the CRLB for Scenario 2 presents a performance limit for "ML – Perfect", which is also designed under the assumption of known indices of malicious LED transmitters. It is noted that the CRLB in the absence of training measurements is a tight limit for the RMSE of the proposed ML estimator only when γ is close to zero or one.

In Fig. 2, the RMSE performance of the estimators is plotted versus the noise level, $10\log_{10}(1/\sigma^2)$. It is observed that the RMSE of the proposed ML estimator in (6) gets close to the CRLB and the RMSE of the "ML – Perfect" as the noise variance decreases. However, the RMSE of "ML – Unaware" estimator does not improve significantly as the noise variance gets lower as it assumes that all the LED transmitters are honest. In addition, it is noticed that for large values of noise variances, the RMSEs of all the estimators are below the CRLBs. This is due to the fact that the possible locations of the VLC receiver in the room are limited to 4×4 meters in two dimensions, and the ML estimators perform the search over this space. On the other hand, the CRLB derivations do not assume any prior information about the location of the VLC receiver; hence, can lead to larger values than RMSEs in very noisy cases.

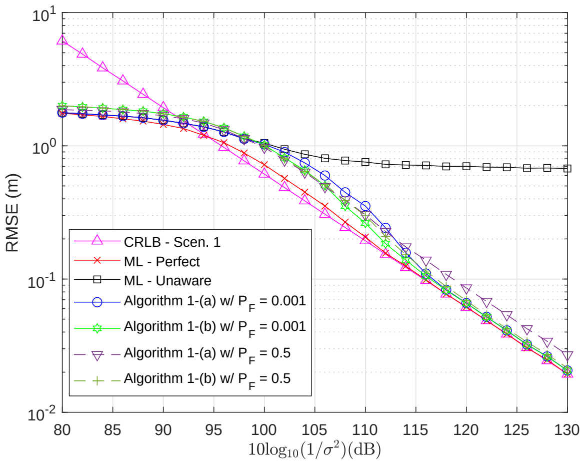


Fig. 3: RMSE versus $10\log_{10}(1/\sigma^2)$ for Scenario 1 ($\gamma = 0.5$).

To evaluate the performance of the algorithms in Section IV-A (Scenario 1), a similar setup is used. The algorithms in this section require a training phase. For this purpose, $N_{\rm V}$ is set to one and the training location is chosen as the center of the room in two dimensions at a height of 0.85 meter, i.e., $(0, 0, 0.85)$ meters. Again, 10^4 different sets of honest and malicious LED realizations are used to obtain average performance results. The same LED transmitter powers as in the previous part are used in both the training and estimation phases since, in Scenario 1, transmit powers of malicious LED transmitters do not change over time. In addition, to set the values of τ_i for the decision rule in (15), a Neyman-Pearson type approach is followed. Namely, for each noise variance σ^2, τ_i's are determined so as to set the false alarm probability of each decision rule to a fixed value of $\rm P_F$ for each LED transmitter. In the simulations, two different values of $\rm P_F$ are considered, namely, $\rm P_F = 0.001$ and $\rm P_F = 0.5$. Based on the obtained thresholds, the conditional error and correct decision probabilities, i.e., ${\rm P}(\widehat{D}_i \,|\, \mathcal{M}_i)$ and ${\rm P}(\widehat{D}_i \,|\, \mathcal{H}_i)$, are calculated using 10^5 Monte-Carlo trials and employed in Algorithm 1-(b). To provide comparisons, the "ML – Perfect" estimator is also considered, which knows not only the malicious LED transmitters but also their transmit powers in this scenario (Scenario 1). Fig. 3 shows the RMSE performance of the algorithms versus the noise level, $10\log_{10}(1/\sigma^2)$, where $\gamma = 0.5$. It is observed that, for $\rm P_F = 0.001$, Algorithm

1-(a) has the same performance as the "ML – Unaware" estimator up to around 100 dB and then gets close to "ML – Perfect" at low noise variances. For $\mathrm{P_F} = 0.5$, Algorithm 1-(a) performs worse than "ML – Unaware" up to around 100 dB but afterwards it achieves lower RMSEs than Algorithm 1-(a) with $\mathrm{P_F} = 0.001$ up to around 113 dB. However, for higher values of $10\log_{10}(1/\sigma^2)$, Algorithm 1-(a) with $\mathrm{P_F} = 0.001$ outperforms Algorithm 1-(a) with $\mathrm{P_F} = 0.5$. Moreover, it is noted from Fig. 3 that the performance of Algorithm 1-(b) is not affected significantly by the false alarm probability $\mathrm{P_F}$ (equivalently, the thresholds). This is because, in Algorithm 1-(b), the probability that an LED transmitter is malicious, γ, is updated based on the observations (see (20)). Thus, Algorithm 1-(b) is robust to changes in the threshold values τ_i as opposed to Algorithm 1-(a), which is a practical advantage.

For performance evaluation of the algorithms in Section IV-B (Scenario 2), 10^4 different sets of honest and malicious LED realizations are employed with a γ value of 0.5. As opposed to Scenario 1, in this scenario, the transmit powers of malicious LEDs are different at each measurement both in the training and estimation phases. Again, N_V is chosen as one by considering the same training point as in the previous case. The training is performed according to the decision rule in (24). To determine the κ_i values, the same approach as in Scenario 1 is taken by setting $\mathrm{P_F} = 0.001$ and $\mathrm{P_F} = 0.5$. Then, based on the κ_i values, the conditional probabilities $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{M}_i)$ and $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{H}_i)$ are calculated using 10^5 Monte-Carlo trials and employed in Algorithm 2-(b). The results in Fig. 4 reveal that for $\mathrm{P_F} = 0.001$, the performance of Algorithm 2-(a) is the same as "ML – Unaware" up to 100 dB and then converges to "ML – Perfect" at low noise variances. However, for $\mathrm{P_F} = 0.5$, Algorithm 2-(a) performs closely to "ML – Perfect" at high noise variances but achieves a significantly inferior performance at low noise variances. In addition, it is observed that the performance of Algorithm 2-(b) is not affected significantly by the false alarm rate $\mathrm{P_F}$ as in Scenario 1. Thus, Algorithm 2-(b) is robust to changes in κ_i values. Based on Fig. 3 and Fig. 4, it can be noted that if the false alarm probability can be adapted according to the noise variance, the performance of Algorithms 1-(a) and Algorithm 2-(a) can be enhanced. Namely, lower (higher) false alarm rates can be chosen for lower (higher) noise variances.

To observe the effects of the VLC receiver position on the accuracy, the VLC receiver is placed $(0, 0, 0.85)$ meters and moved along the straight line towards the location $(1, 1, 0.85)$ meters, where γ is set to 0.5. The simulations are conducted for two different values of the noise variance, namely, $\sigma^2 = 10^{-11}$ and $\sigma^2 = 10^{-12}$. In Fig. 5-(a), Algorithm 1-(a) achieves lower RMSEs with $\mathrm{P_F} = 0.5$ than with $\mathrm{P_F} = 0.001$. Conversely, in Fig. 5-(b), Algorithm 1-(a) with $\mathrm{P_F} = 0.001$ outperforms that with $\mathrm{P_F} = 0.5$. On the other hand, the RMSE performances of Algorithm 1-(b) are very similar at both false alarm probabilities due to its probability update operation, as discussed previously. In addition, it is observed that the RMSEs of the estimators get larger as the VLC receiver moves away from the center. This simulation is repeated for Scenario 2 and the results are presented in Fig. 6. In Fig. 6-(a), Algorithm 2-(a) with $\mathrm{P_F} = 0.5$ performs better than Algorithm 2-(a) with $\mathrm{P_F} = 0.001$. On the contrary, in Fig. 6-(b), Algorithm 2-(a) with $\mathrm{P_F} = 0.5$ performs poorly as the VLC receiver moves away from the center, whereas Algorithm 2-(a) with $\mathrm{P_F} = 0.001$ performs closely to the CRLB. Again, Algorithm 1-(b) achieves very similar RMSEs for both false alarm probabilities and the RMSE values of the estimators and the CRLB tend to increase as the VLC receiver moves away from the center of the room. These results illustrate the robustness of Algorithm 1-(b) and Algorithm 2-(b) against the threshold values used in the detection step. In addition, Algorithm 1-(a) and Algorithm 2-(a) are observed to be sensitive to the threshold values, and it is concluded that lower false alarm probabilities should be used for setting their thresholds as the noise level decreases; i.e., the SNR increases.

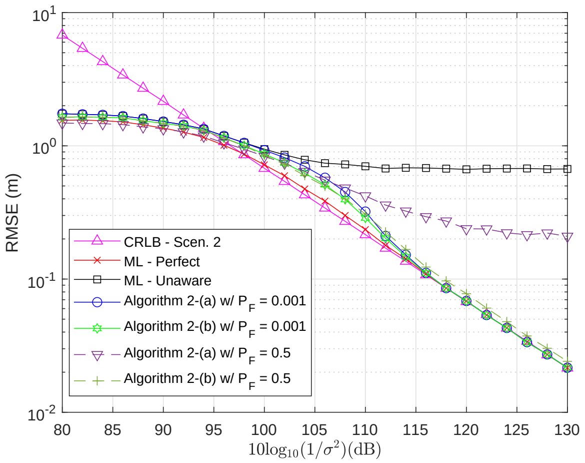


Fig. 4: RMSE versus $10\log_{10}(1/\sigma^2)$ for Scenario 2 ($\gamma = 0.5$).

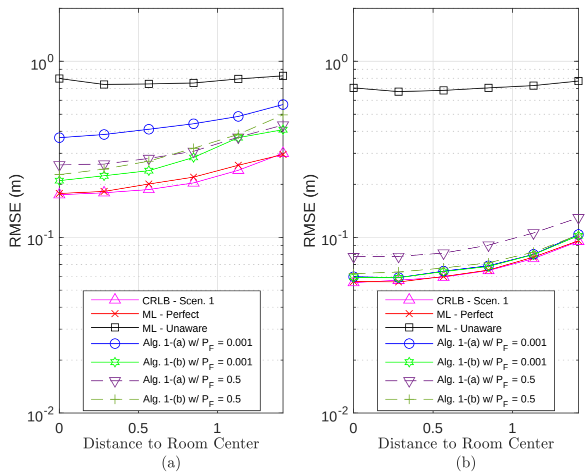
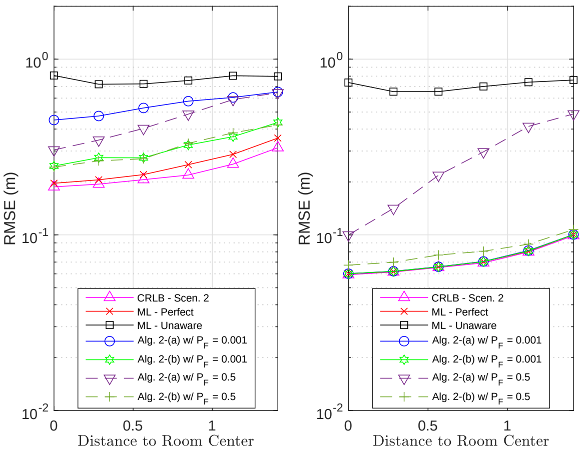


Fig. 5: For Scenario 1, RMSE versus distance of VLC receiver from location $(0, 0, 0.85)$ m, where $\gamma = 0.5$ and VLC receiver moves on the straight line towards $(1, 1, 0.85)$ m. (a) $\sigma^2 = 10^{-11}$, (b) $\sigma^2 = 10^{-12}$.

Moreover, the UMP test proposed in Section IV-C for Scenario 1 can be investigated as the $P_{\mathrm{M},i}$ values are lower than or equal to $P_{\mathrm{H},i}$, $\forall i$ for the considered setting (namely, $P_{\mathrm{M},i} \in [1\,W, 3\,W]$ and $P_{\mathrm{H},i} = 5\,\mathrm{W}$); hence, the condition in (28) is satisfied. The false alarm probability is set to 0.5 in the simulations to highlight the advantage of employing the UMP test. It can be seen from Fig. 7 that the UMP test specified by (31) and (35) achieves higher detection



(a)

(b)

Fig. 6: For Scenario 2, RMSE versus distance of VLC receiver from location $(0, 0, 0.85)$ m, where $\gamma = 0.5$ and VLC receiver moves on the straight line towards $(1, 1, 0.85)$ m. (a) $\sigma^2 = 10^{-11}$, (b) $\sigma^2 = 10^{-12}$.

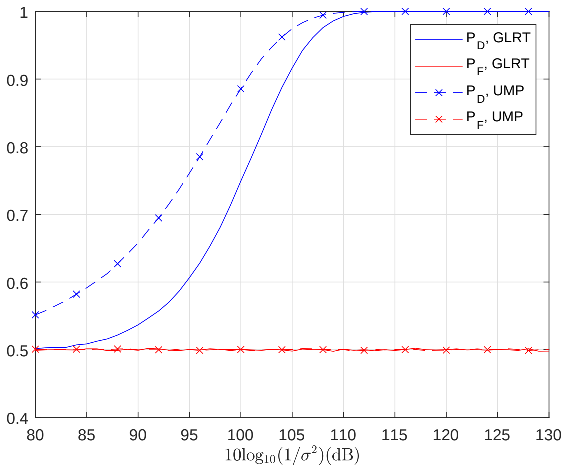


Fig. 7: Detection and false alarm probabilities of the GLRT and UMP tests versus $10\log_{10}(1/\sigma^2)$ for $P_F = 0.5$.

probabilities than the GLRT in (15) for the large values of the noise variances while keeping the false alarm probability the same. Thus, the UMP test can lead to improved RMSE performance at high noise levels. In Fig. 8, it is observed that Algorithm 1-(a) that utilizes the UMP test, labeled as “Algorithm 1-(a), UMP”, outperforms Algorithm 1-(a), which employs the GLRT test. Hence, enhanced localization accuracy can be achieved via the UMP test when the condition in (28) is satisfied. However, Algorithm 1-(b) with the UMP test, labeled as “Algorithm 1-(b), UMP”, does not provide significant performance improvements since Algorithm 1-(b) is robust to the changes in the τ_i values.

Furthermore, we conduct simulations to investigate the effects of the number of training locations, i.e., $N_{\rm V}$, used in the algorithms in Sec. IV on the positioning accuracy. The noise variance is fixed as $10\log_{10}(1/\sigma^2) = 110$ dB to illustrate the effects of increasing the number of training locations. The value of $N_{\rm V}$ is changed from 1 to 16 while keeping the rest of the parameters the same. For the choice of training locations, we employ a uniform grid array in two dimensions

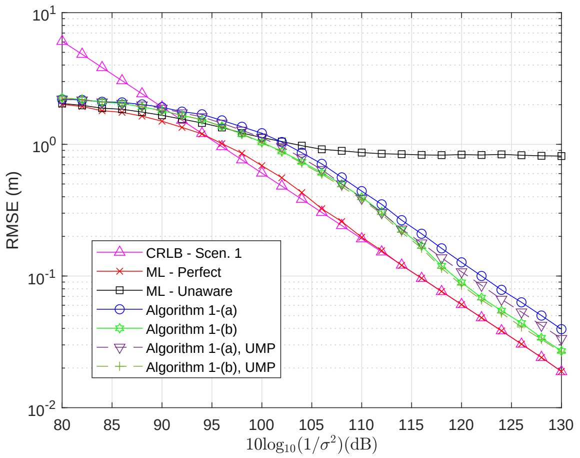


Fig. 8: RMSE versus $10\log_{10}(1/\sigma^2)$ for Scenario 1 ($\gamma = 0.5$).

at a height of 0.85 meter across the room for each $N_{\rm V}$.[2] It is observed from Fig. 9 that for the false alarm rate of 0.001, Algorithm 1-(a) is outperformed by Algorithm 1-(b) when $N_{\rm V}$ is small; however, it achieves lower RMSEs than Algorithm 1-(b) and converges to the performance of the ML estimator that perfectly knows the transmit powers of the malicious LEDs (labeled as “ML – Perfect”) as $N_{\rm V}$ increases. Similarly, when the false alarm rate is 0.5, Algorithm 1-(b) has better (worse) positioning accuracy than Algorithm 1-(a) for small (large) values of $N_{\rm V}$. In general, it is noted that from Fig. 9 that after the value of $N_{\rm V} = 8$, there are not any significant improvements in the performance of the algorithms. A similar simulation is also performed for Scenario 2 in Sec. IV-B with the same parameters. It can be seen from Fig. 10 that for the false alarm rate of 0.001, Algorithm 2-(a) is outperformed by Algorithm 2-(b) when $N_{\rm V}$ is small; however, it achieves lower RMSEs than Algorithm 2-(b) as $N_{\rm V}$ increases. On the other hand, when the false alarm rate is 0.5, Algorithm 2-(b) outperforms Algorithm 2-(a) for all values of $N_{\rm V}$, and its performance is not affected significantly by the number of training locations. Similar to Scenario 1, the performances of the algorithms do not have any significant improvements after the value of $N_{\rm V} = 6$ in Scenario 2.

VII. Extension to the Case of Unknown γ_i's

In this section, we consider the case in which the probabilities of the LED transmitters being malicious, i.e., $\gamma_1, \ldots, \gamma_{N_{\rm L}}$, are unknown. Let z_i denote whether the ith LED transmitter is malicious or not; that is,

$$z_i = \begin{cases} 0\,, & \text{if } i\text{th LED is honest} \\ 1\,, & \text{if } i\text{th LED is malicious} \end{cases} \tag{66}$$

which is a Bernoulli random variable with parameter γ_i. Then, using the definition in (2), $P_{{\rm T},i}$ can be expressed as

$$P_{{\rm T},i} = (1 - z_i)P_{{\rm H},i} + z_i P_{{\rm M},i} \tag{67}$$

In this case, the unknown parameters are $\boldsymbol{l}_{\rm R}$, $\boldsymbol{P}_{\rm M}$, and $\boldsymbol{z}$, where $\boldsymbol{z}$ denotes the vector of z_i values for $i = 1, \ldots, N_{\rm L}$.

[2] Obtaining the optimum arrangement of training locations can be considered as an important theoretical problem, which is out of scope of this work.

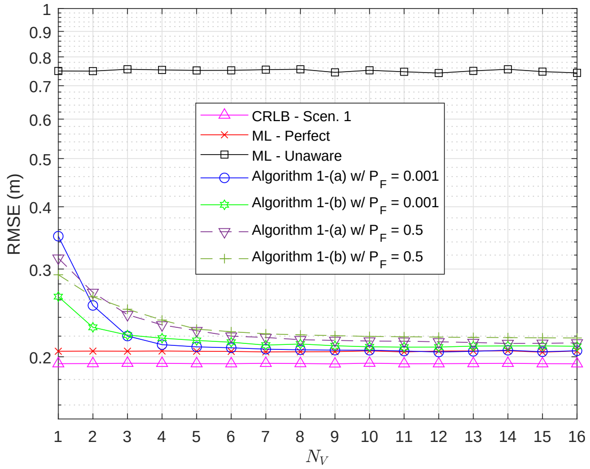


Fig. 9: RMSE versus N_{V} in Scenario 1 for $10\log_{10}(1/\sigma^2) = 110$ dB.

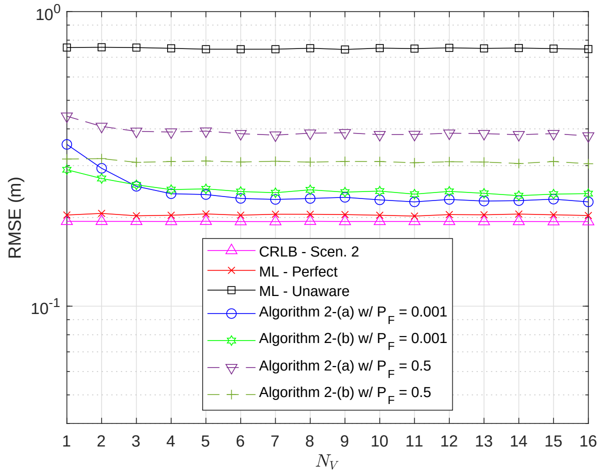


Fig. 10: RMSE versus N_{V} in Scenario 2 for $10\log_{10}(1/\sigma^2) = 110$ dB.

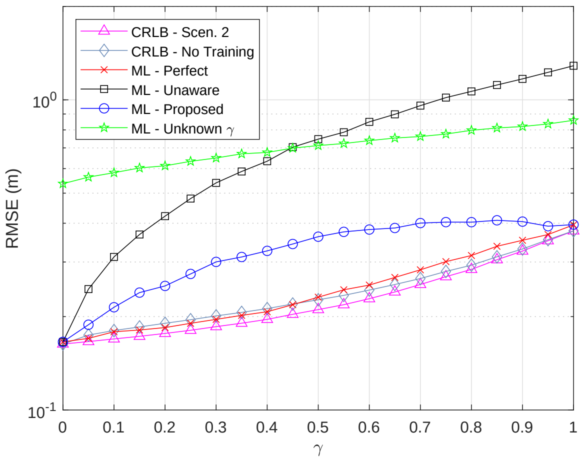


Fig. 11: RMSE versus γ for $\sigma^2 = 10^{-11}$.

Thus, the likelihood function of $\boldsymbol{P}_{\mathrm{R}}$ given these parameters can be stated as

$$p(\boldsymbol{P}_{\mathrm{R}}|\boldsymbol{l}_{\mathrm{R}}, \boldsymbol{P}_{\mathrm{M}}, \boldsymbol{z}) = \prod_{i\in H_{\boldsymbol{z}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{H},i}R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} \times \prod_{i\in M_{\boldsymbol{z}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{M},i}R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} \tag{68}$$

where sets $H_{\boldsymbol{z}}$ and $M_{\boldsymbol{z}}$ are defined as

$$H_{\boldsymbol{z}} = \{i \in \{1, \ldots, N_{\mathrm{L}}\} \,|\, z_i = 0\} \tag{69}$$

$$M_{\boldsymbol{z}} = \{i \in \{1, \ldots, N_{\mathrm{L}}\} \,|\, z_i = 1\} \tag{70}$$

Then, for the estimation without a training phase (as in Section III) in the case of unknown γ_i's, the following ML estimator is derived:

$$(\widehat{\boldsymbol{l}}_{\mathrm{R}}, \widehat{\boldsymbol{P}}_{\mathrm{M}}, \widehat{\boldsymbol{z}}) = \arg\max_{\boldsymbol{l}_{\mathrm{R}}, \boldsymbol{P}_{\mathrm{M}}, \boldsymbol{z}} p(\boldsymbol{P}_{\mathrm{R}}|\boldsymbol{l}_{\mathrm{R}}, \boldsymbol{P}_{\mathrm{M}}, \boldsymbol{z}) \tag{71}$$

$$= \arg\min_{\boldsymbol{l}_{\mathrm{R}}, \boldsymbol{z}} \sum_{i\in H_{\boldsymbol{z}}} \frac{(P_{\mathrm{R},i} - P_{\mathrm{H},i}R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{\sigma_i^2} + \sum_{i\in M_{\boldsymbol{z}}} \frac{(P_{\mathrm{R},i} - \widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_{\mathrm{R}}) R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{\sigma_i^2} \tag{72}$$

where $\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_{\mathrm{R}})$ for any $\boldsymbol{z}$ is given by

$$\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_{\mathrm{R}}) = \begin{cases} P_{\min,i}, & \text{if } \frac{P_{\mathrm{R},i}}{R_p h_i(\boldsymbol{l}_{\mathrm{R}})} \leq P_{\min,i} \\ P_{\max,i}, & \text{if } \frac{P_{\mathrm{R},i}}{R_p h_i(\boldsymbol{l}_{\mathrm{R}})} \geq P_{\max,i} \\ \frac{P_{\mathrm{R},i}}{R_p h_i(\boldsymbol{l}_{\mathrm{R}})}, & \text{otherwise} \end{cases} \tag{73}$$

It should be noted that there are 2^{N_L} possible values of $z_1, \ldots, z_{N_{\mathrm{L}}}$. Hence, the ML estimator in (72) has high computational complexity for large values of N_{L}.

To evaluate the performance of the proposed ML estimator for the case of unknown γ_i's, simulations are conducted for the setting in Section VI considering no training measurements. The results in Fig. 11 illustrate that without the knowledge of γ, the positioning accuracy can degrade significantly for all values of γ compared to the proposed ML estimator in (6) for the case of known γ.

VIII. Extension to Cases with All or None of LEDs being Malicious

In this part, we extend the results in Sections III and IV to cover a different case. Namely, it is assumed that when a hijacking event occurs, the malicious third party accesses the VLP controller and makes all the LED transmitters malicious (i.e., modifies all the power levels). Let the probability of such a hijacking event be denoted by γ. Then, the probability distribution of the received powers from the LED transmitters in (1) for given values of the unknown position and malicious power levels can be expressed as follows (cf. (5)):

$$p(\boldsymbol{P}_{\mathrm{R}}\,|\,\boldsymbol{l}_{\mathrm{R}},\boldsymbol{P}_{\mathrm{M}}) = \gamma\prod_{i=1}^{N_{\mathrm{L}}}\frac{1}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{M},i}R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} + (1-\gamma)\prod_{i=1}^{N_{\mathrm{L}}}\frac{1}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{H},i}R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} \tag{74}$$

Then, the ML estimator for the location of the VLC receiver is obtained as

$$\widehat{\boldsymbol{l}}_{\mathrm{R}} = \underset{\boldsymbol{l}_{\mathrm{R}}\in\mathcal{L}}{\arg\max}\;\gamma\prod_{i=1}^{N_{\mathrm{L}}}\frac{1}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_{\mathrm{R}})R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} + (1-\gamma)\prod_{i=1}^{N_{\mathrm{L}}}\frac{1}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{H},i}R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}}$$

where $\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_{\mathrm{R}})$ is as in (7). In addition, if there exist training measurements, then a single hypothesis-testing problem can be formulated for Scenario 2 (instead of the N_{L} separate problems in (22)) as follows:

$$\begin{aligned}\mathcal{H}\;&:\;P_{\mathrm{R},i}^{(j)} = R_p\,P_{\mathrm{H},i}\,h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)+\eta_i^{(j)},\\ \mathcal{M}\;&:\;P_{\mathrm{R},i}^{(j)} = R_p\,P_{\mathrm{M},i}^{(j)}\,h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)+\eta_i^{(j)},\end{aligned} \tag{75}$$

for $j=1,\ldots,N_{\mathrm{V}}$ and $i=1,\ldots N_{\mathrm{L}}$ under each hypothesis, where $P_{\mathrm{M},i}^{(j)}$ becomes $P_{\mathrm{M},i}$ in Scenario 1 (cf., the N_{L} separate problems in (11)). Then, the GLRT can be formulated as

$$\frac{\displaystyle\max_{\{P_{\mathrm{M},i}^{(j)}\}}\prod_{i=1}^{N_{\mathrm{L}}}\prod_{j=1}^{N_{\mathrm{V}}}\frac{1}{\sqrt{2\pi}\sigma_{i,j}}e^{-\frac{\left(P_{\mathrm{R},i}^{(j)}-R_pP_{\mathrm{M},i}^{(j)}h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}}{\displaystyle\prod_{i=1}^{N_{\mathrm{L}}}\prod_{j=1}^{N_{\mathrm{V}}}\frac{1}{\sqrt{2\pi}\sigma_{i,j}}e^{-\frac{\left(P_{\mathrm{R},i}^{(j)}-R_pP_{\mathrm{H},i}h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}}\;\underset{\mathcal{H}}{\overset{\mathcal{M}}{\gtrless}}\;\kappa \tag{76}$$

which can be simplified into the following rule for Scenario 2 (cf. (24)):

$$\sum_{i=1}^{N_{\mathrm{L}}}\sum_{j=1}^{N_{\mathrm{V}}}\frac{1}{\sigma_{i,j}^2}\Big(R_pP_{\mathrm{R},i}^{(j)}h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big(\widehat{P}_{\mathrm{M},i}^{(j)}-P_{\mathrm{H},i}\big) + 0.5R_p^2\big(h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big)^2\Big(P_{\mathrm{H},i}^2-\big(\widehat{P}_{\mathrm{M},i}^{(j)}\big)^2\Big)\Big)\;\underset{\mathcal{H}}{\overset{\mathcal{M}}{\gtrless}}\;\log(\kappa)$$

where $\widehat{P}_{\mathrm{M},i}^{(j)}$ is as in (25) and κ is the threshold parameter. Also, in Scenario 1, $P_{\mathrm{M},i}^{(j)}$ is set to $P_{\mathrm{M},i}$, and (76) is simplified as (cf. (15))

$$\sum_{i=1}^{N_{\mathrm{L}}}\Bigg(R_p\big(\widehat{P}_{\mathrm{M},i}-P_{\mathrm{H},i}\big)\sum_{j=1}^{N_{\mathrm{V}}}\frac{P_{\mathrm{R},i}^{(j)}h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)}{\sigma_{i,j}^2} + 0.5R_p^2\Big(P_{\mathrm{H},i}^2-\big(\widehat{P}_{\mathrm{M},i}\big)^2\Big)\sum_{j=1}^{N_{\mathrm{V}}}\frac{\big(h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big)^2}{\sigma_{i,j}^2}\Bigg)\;\underset{\mathcal{H}}{\overset{\mathcal{M}}{\gtrless}}\;\log(\kappa)$$

where $\widehat{P}_{\mathrm{M},i}$ is as in (13) and (14).

In this case, when the decision is hypothesis $\mathcal{M}$, no localization is performed since all the power levels are classified as incorrect (manipulated). This can be regarded as an *outage* event. When the decision is $\mathcal{H}$, localization is performed based on (1) with $P_{\mathrm{T},i}=P_{\mathrm{H},i}$ for all $i\in\{1,\ldots,N_{\mathrm{L}}\}$, which leads to the "ML – Unaware" estimator in Section VI. Hence, the main ideas in Sections III and IV can also be employed for the case in which a malicious third party aims to modify the power levels of all the LED transmitters.

IX. Concluding Remarks

In this manuscript, position estimation problems have been formulated for VLP systems in the presence of malicious LED transmitters for the first time in the literature. An ML estimator has been derived based on the knowledge of probabilities that LED transmitters can be malicious. In addition, in the presence of training measurements, GLRTs have been employed for detection of malicious LED transmitters, and based on the decisions of the GLRTs, various ML based location estimators have been developed. Moreover, CRLB expressions have been derived and used as benchmarks to evaluate the performance of the proposed estimators. Finally, an ML estimator has been proposed for the case that the probabilities of the LED transmitters being malicious are unknown.

As possible directions for future work, uncertainties in the knowledge of the probabilities that the LED transmitters are malicious (i.e., γ_i's) can be considered. Also, more general channel models that take into account reflected and/or diffused components (in addition to the line-of-sight component) can be employed. In addition, information theoretic learning criteria such as MEE and MCC can be used for VLP systems in the presence of malicious LED transmitters to develop new approaches. Furthermore, possible ways of dealing with the presence of malicious LED transmitters, such as power allocation, can be developed.

For the analyses in this study, the noise components (i.e., η_i in (1)) are modeled to be independent of received signal powers, which is a valid assumption when shot noise is negligible compared to thermal noise. (In the simulation setup in Section VI, the shot noise is negligible.) When the received power levels are high, shot noise can be important and the variances of the Gaussian noise components in (1) can depend on the received signal powers [47], [48]. In this case, the position estimation approaches in this paper can be extended as follows: Let the variance of the zero-mean Gaussian noise component η_i in (1) be denoted by $\tilde{\sigma}_i^2$, which is expressed as the sum of the variances of the thermal and shot noise components [48]. That is,

$$\tilde{\sigma}_i^2 = \sigma_i^2 + \varsigma R_p P_{\mathrm{T},i}h_i(\boldsymbol{l}_{\mathrm{R}}) \tag{77}$$

where σ_i^2 is the variance of the thermal noise component, ς is a constant for the variance of the shot noise component [47], and the other terms are as defined in Section II. Based on this model, the ML estimator in Section III can be updated as follows (cf. (4) and (5)):

$$\Big(\widehat{\boldsymbol{l}}_{\mathrm{R}},\widehat{\boldsymbol{P}}_{\mathrm{M}}\Big) = \underset{\boldsymbol{l}_{\mathrm{R}}\in\mathcal{L},\boldsymbol{P}_{\mathrm{M}}\in\mathcal{P}}{\arg\max}\prod_{i=1}^{N_{\mathrm{L}}}\Bigg(\frac{\gamma_i\,e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{M},i}R_ph_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2(\sigma_i^2+\varsigma R_pP_{\mathrm{M},i}h_i(\boldsymbol{l}_{\mathrm{R}}))}}}{\sqrt{2\pi(\sigma_i^2+\varsigma R_pP_{\mathrm{M},i}h_i(\boldsymbol{l}_{\mathrm{R}}))}} + \frac{(1-\gamma_i)e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{H},i}R_ph_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2(\sigma_i^2+\varsigma R_pP_{\mathrm{H},i}h_i(\boldsymbol{l}_{\mathrm{R}}))}}}{\sqrt{2\pi(\sigma_i^2+\varsigma R_pP_{\mathrm{H},i}h_i(\boldsymbol{l}_{\mathrm{R}}))}}\Bigg) \tag{78}$$

Since each $P_{\mathrm{M},i}$ can be optimized separately for a given $\boldsymbol{l}_\mathrm{R}$, it is also possible to determine the optimal values of $P_{\mathrm{M},i}$ in terms of $\boldsymbol{l}_\mathrm{R}$ (called $\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_\mathrm{R})$) and obtain a simplified version of the ML estimator (similarly to (6)). For the position estimation approaches in the presence of training measurements in Section IV, extensions based on the updated variance formula in (77) can be performed in a straightforward manner. For example, the GLRT in (12) can be updated by replacing $\sigma_{i,j}^2$'s in the numerator by $\sigma_{i,j}^2 + \varsigma R_p P_{\mathrm{M},i} h_i(\boldsymbol{l}_\mathrm{R}^{(j)})$ and those in the denominator by $\sigma_{i,j}^2 + \varsigma R_p P_{\mathrm{H},i} h_i(\boldsymbol{l}_\mathrm{R}^{(j)})$.

References

[1] F. Kokdogan and S. Gezici, "Position estimation in visible light systems in the presence of malicious LED transmitters," in *IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, May 2021, pp. 1–6.

[2] M. Yoshino, S. Haruyama, and M. Nakagawa, "High-accuracy positioning system using visible LED lights and image sensor," in *2008 IEEE Radio and Wireless Symposium*, 2008, pp. 439–442.

[3] J. Luo, L. Fan, and H. Li, "Indoor positioning systems based on visible light communication: State of the art," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2871–2893, 4th Quart. 2017.

[4] M. F. Keskin, A. D. Sezer, and S. Gezici, "Localization via visible light systems," *Proceedings of the IEEE*, vol. 106, no. 6, pp. 1063–1088, June 2018.

[5] J. Armstrong, Y. A. Sekercioglu, and A. Neild, "Visible light positioning: a roadmap for international standardization," *IEEE Communications Magazine*, vol. 51, no. 12, pp. 68–73, 2013.

[6] H. Steendam, T. Q. Wang, and J. Armstrong, "Cramer-Rao bound for AOA-based VLP with an aperture-based receiver," in *2017 IEEE International Conference on Communications (ICC)*, 2017, pp. 1–6.

[7] M. F. Keskin, S. Gezici, and O. Arikan, "Direct and two-step positioning in visible light systems," *IEEE Transactions on Communications*, vol. 66, no. 1, pp. 239–254, Jan. 2018.

[8] B. Zhou, A. Liu, and V. Lau, "On the fundamental performance limit of visible light-based positioning," in *2019 13th International Conference on Signal Processing and Communication Systems (ICSPCS)*, 2019, pp. 1–6.

[9] S.-H. Yang, H.-S. Kim, Y.-H. Son, and S.-K. Han, "Three-dimensional visible light indoor localization using AOA and RSS with multiple optical receivers," *Journal of Lightwave Technology*, vol. 32, no. 14, pp. 2480–2485, July 2014.

[10] S. Shen, S. Li, and H. Steendam, "Simultaneous position and orientation estimation for visible light systems with multiple LEDs and multiple PDs," *IEEE Journal on Selected Areas in Communications*, vol. 38, no. 8, pp. 1866–1879, 2020.

[11] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, C. M. Assi, M. Safari, and H. Haas, "Invoking deep learning for joint estimation of indoor LiFi user position and orientation," *IEEE Journal on Selected Areas in Communications*, vol. 39, no. 9, pp. 2890–2905, 2021.

[12] H. Steendam, T. Q. Wang, and J. Armstrong, "Theoretical lower bound for indoor visible light positioning using received signal strength measurements and an aperture-based receiver," *Journal of Lightwave Technology*, vol. 35, no. 2, pp. 309–319, 2017.

[13] G. Blinowski, "Security of visible light communication systems-A survey," *Physical Communication*, vol. 34, pp. 246–260, June 2019.

[14] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *IEEE Globecom Workshops (GC Wkshps)*, 2014, pp. 524–529.

[15] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communications with spatial jamming," in *IEEE International Conference on Communications (ICC)*, 2019, pp. 1–6.

[16] F. Wang, C. Liu, Q. Wang, J. Zhang, R. Zhang, L. Yang, and L. Hanzo, "Optical jamming enhances the secrecy performance of the generalized space-shift-keying-aided visible-light downlink," *IEEE Transactions on Communications*, vol. 66, no. 9, pp. 4087–4102, Sep. 2018.

[17] H. Shen, Y. Deng, W. Xu, and C. Zhao, "Secrecy-oriented transmitter optimization for visible light communication systems," *IEEE Photonics Journal*, vol. 8, no. 5, pp. 1–14, 2016.

[18] S. Cho, G. Chen, and J. P. Coon, "Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 10, pp. 2633–2648, 2019.

[19] L. Qian, X. Chi, L. Zhao, and A. Chaaban, "Secure visible light communications via intelligent reflecting surfaces," in *ICC 2021 - IEEE International Conference on Communications*, 2021, pp. 1–6.

[20] M. A. Arfaoui, Z. Rezki, A. Ghrayeb, and M. S. Alouini, "On the secrecy capacity of MISO visible light communication channels," in *IEEE Global Communications Conference*, 2016, pp. 1–7.

[21] H. Abumarshoud, M. D. Soltani, M. Safari, and H. Haas, "Secrecy capacity of LiFi systems," in *Emerging Imaging and Sensing Technologies for Security and Defence V; and Advanced Manufacturing Technologies for Micro- and Nanosystems in Security and Defence III*, vol. 11540. SPIE, 2020, pp. 127–137.

[22] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, "Physical layer security for visible light communication systems: A survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1887–1908, 2020.

[23] R. Mitra and V. Bhatia, "Minimum error entropy criterion based channel estimation for massive-MIMO in VLC," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 1, pp. 1014–1018, 2019.

[24] A. Vempaty, O. Ozdemir, K. Agrawal, H. Chen, and P. K. Varshney, "Localization in wireless sensor networks: Byzantines and mitigation techniques," *IEEE Transactions on Signal Processing*, vol. 61, no. 6, pp. 1495–1508, 2013.

[25] X. Mei, H. Wu, J. Xian, and B. Chen, "RSS-based Byzantine fault-tolerant localization algorithm under NLOS environment," *IEEE Communications Letters*, vol. 25, no. 2, pp. 474–478, 2021.

[26] R. Niu, A. Vempaty, and P. K. Varshney, "Received-signal-strength-based localization in wireless sensor networks," *Proceedings of the IEEE*, vol. 106, no. 7, pp. 1166–1182, 2018.

[27] A. Vempaty, Y. S. Han, and P. K. Varshney, "Byzantine tolerant target localization in wireless sensor networks over non-ideal channels," in *13th International Symposium on Communications and Information Technologies*, 2013, pp. 407–411.

[28] ——, "Target localization in wireless sensor networks using error correcting codes," *IEEE Transactions on Information Theory*, vol. 60, no. 1, pp. 697–712, 2014.

[29] S. K. Saini and P. Singh, "Analysis and detection of Byzantine attack in wireless sensor network," in *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, 2016, pp. 3189–3191.

[30] A. Vempaty, O. Ozdemir, and P. K. Varshney, "Target tracking in wireless sensor networks in the presence of Byzantines," in *Proceedings of the 16th International Conference on Information Fusion*, 2013, pp. 968–973.

[31] Q. Yu, H. Chen, and L. Xie, "A modified distributed target localization scheme in the presence of Byzantine attack," in *2015 International Conference on Wireless Communications Signal Processing (WCSP)*, 2015, pp. 1–5.

[32] P. Zhang, S. G. Nagarajan, and I. Nevat, "Secure location of things (SLOT): Mitigating localization spoofing attacks in the internet of things," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2199–2206, 2017.

[33] M. Prakruthi and M. Varalatchoumy., "Detecting malicious beacon nodes for secure localization in distributed wireless networks," in *3rd International Conference on Advances in Recent Technologies in Communication and Computing (ARTCom 2011)*, 2011, pp. 206–208.

[34] E. Gonendik and S. Gezici, "Fundamental limits on RSS based range estimation in visible light positioning systems," *IEEE Communications Letters*, vol. 19, no. 12, pp. 2138–2141, Dec. 2015.

[35] M. F. Keskin, A. D. Sezer, and S. Gezici, "Optimal and robust power allocation for visible light positioning systems under illumination constraints," *IEEE Transactions on Communications*, vol. 67, no. 1, pp. 527–542, 2019.

[36] D. Karunatilaka, F. Zafar, V. Kalavally, and R. Parthiban, "LED based indoor visible light communications: State of the art," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1649–1678, 3rd Quart. 2015.

[37] S. D. Lausnay, L. D. Strycker, J. P. Goemaere, B. Nauwelaers, and N. Stevens, "A survey on multiple access visible light positioning," in *IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech)*, Aug. 2016, pp. 38–42.

[38] T. Wang, Y. Sekercioglu, A. Neild, and J. Armstrong, "Position accuracy of time-of-arrival based ranging using visible light with application in

indoor localization systems," *Journal of Lightwave Technology*, vol. 31, no. 20, pp. 3302–3308, Oct. 2013.

[39] A. Sahin, Y. S. Eroglu, I. Guvenc, N. Pala, and M. Yuksel, "Hybrid 3-D localization for visible light communication systems," *Journal of Lightwave Tech.*, vol. 33, no. 22, pp. 4589–4599, Nov. 2015.

[40] J. M. Kahn and J. R. Barry, "Wireless infrared communications," *Proceedings of the IEEE*, vol. 85, no. 2, pp. 265–298, Feb. 1997.

[41] D. Plets, S. Bastiaens, L. Martens, W. Joseph, and N. Stevens, "On the impact of LED power uncertainty on the accuracy of 2D and 3D visible light positioning," *Optik*, vol. 195, p. 163027, 2019.

[42] L. Thomas and R. Markus, "Reliability and lifetime of LEDs," *OSRAM Opto Semiconductors, Application Note*, no. AN006, 2020.

[43] M.-H. Chang, D. Das, P. Varde, and M. Pecht, "Light emitting diodes reliability review," *Microelectronics Reliability*, vol. 52, no. 5, pp. 762–782, 2012.

[44] H. V. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1994.

[45] C. Robert and G. Casella, *Monte Carlo Statistical Methods*. Springer Verlag, 2004.

[46] M. F. Keskin and S. Gezici, "Comparative theoretical analysis of distance estimation in visible light positioning systems," *Journal of Lightwave Technology*, vol. 34, no. 3, pp. 854–865, Feb. 2016.

[47] X. Liu, D. Zou, N. Huang, and S. Zhang, "A comprehensive accuracy analysis of visible light positioning under shot noise," in *2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, 2020, pp. 167–172.

[48] A. Cheema, M. Alsmadi, and S. Ikki, "Effect of signal-dependent shot noise on visible light positioning," *IEEE Photonics Journal*, vol. 14, no. 3, pp. 1–7, 2022.

Furkan Kokdogan received his B.S. and M.S. degrees from the Department of Electrical and Electronics Engineering, Bilkent University, Ankara, Turkey in 2015 and 2017 respectively. He is currently pursuing his Ph.D. in the same department. He has been with ASML Netherlands B.V., Veldhoven, where he works as an Embedded Logic and Firmware Designer since 2022. His current research interest is visible light positioning.

Sinan Gezici (S'03–M'06–SM'11) received the B.Sc. degree in electrical and electronics engineering from Bilkent University, Ankara, Turkey, in 2001, and the Ph.D. degree in electrical engineering from Princeton University, Princeton, NJ, USA, in 2006. From 2006 to 2007, he worked at Mitsubishi Electric Research Laboratories, Cambridge, MA, USA. Since 2007, he has been with the Department of Electrical and Electronics Engineering at Bilkent University, where he is currently a Professor. Dr. Gezici's research interests are in the areas of detection and estimation theory, wireless communications, and localization systems. Among his publications in these areas is the book Ultra-wideband Positioning Systems: Theoretical Limits, Ranging Algorithms, and Protocols (Cambridge University Press, 2008). Dr. Gezici has been an associate editor for IEEE Transactions on Vehicular Technology, IEEE Transactions on Communications, IEEE Wireless Communications Letters, and Journal of Communications and Networks.