2021 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom) | 978-1-6654-0308-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/BlackSeaCom52164.2021.9527842

Position Estimation in Visible Light Systems in the Presence of Malicious LED Transmitters

Furkan Kokdogan and Sinan Gezici
Department of Electrical and Electronics Engineering, Bilkent University, Ankara, Turkey
Emails: {kokdogan, gezici}@ee.bilkent.edu.tr

***Abstract*—We focus on 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.**

***Keywords:* Visible light, estimation, localization, malicious LED transmitter.**

I. Introduction

Recently, 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 [1], [2] (and references therein). Unlike in RF systems, position estimation based on received power measurements can achieve high accuracy in VLP systems [3]. Therefore, the received power parameter is commonly employed in VLP systems due to its low measurement cost.

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 light emitting diode (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 [4]–[11], there exists no such work for VLP systems in the literature. For example, [5] 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 [8], 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 addition, the studies in [10] and [11] focus on the calculation of the secrecy capacity for VLC systems in various scenarios.

In RF systems, position estimation in wireless sensor networks in the presence of malicious nodes has been considered in various studies such as [12] and [13]. However, the proposed approaches are not directly applicable to VLP systems which carry significant differences from RF based positioning systems due to distinct propagation characteristics. 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.

In addition, simulation results are presented to investigate the performance of the proposed algorithms.

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.

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

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

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 $j \neq i$ [14].

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

978-1-6654-0308-5/21/$31.00 ©2021 IEEE

party) and $P_{\mathrm{H},i}$ represents the transmit power of the ith LED transmitter if it is honest (i.e., not malicious). The parameters $\{P_{\mathrm{H},i}\}_{i=1}^{N_\mathrm{L}}$ 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, $\{P_{\mathrm{M},i}\}_{i=1}^{N_\mathrm{L}}$ 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 [2], [15], [16], the channel coefficients in (1) can be calculated as

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

where m_i is the Lambertian order for the ith LED transmitter, A_R is the area of the PD at the VLC receiver, and $\boldsymbol{n}_\mathrm{R}$ and $\boldsymbol{n}_\mathrm{T}^i$ represent the orientation vectors of the VLC receiver and the ith LED transmitter, respectively [17]. It is assumed that the VLC receiver knows the parameters A_R, R_p, $\boldsymbol{n}_\mathrm{R}$, m_i, $\boldsymbol{l}_\mathrm{T}^i$, and $\boldsymbol{n}_\mathrm{T}^i$, and σ_i^2 [3], [16]. For example, the orientation of the VLC receiver ($\boldsymbol{n}_\mathrm{R}$) can be determined by a gyroscope and the LED parameters (m_i, $\boldsymbol{l}_\mathrm{T}^i$, and $\boldsymbol{n}_\mathrm{T}^i$) can be sent to the receiver via visible light communications [3].

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 $\boldsymbol{l}_\mathrm{T}^i$, $\boldsymbol{n}_\mathrm{T}^i$, and m_i as their modification requires physical intervention to the system.

III. Position Estimation in the Presence of Malicious LED Transmitters

The aim of the VLC receiver is to estimate its location $\boldsymbol{l}_\mathrm{R}$ based on the power measurements in (1). Let $\boldsymbol{P}_\mathrm{R}$ represent a vector consisting of the power measurements; i.e., $\boldsymbol{P}_\mathrm{R} = [P_{\mathrm{R},1}\cdots P_{\mathrm{R},N_\mathrm{L}}]^T$. Also, let $\boldsymbol{P}_\mathrm{M}$ denote the vector of unknown transmit powers in (2); that is, $\boldsymbol{P}_\mathrm{M} = [P_{\mathrm{M},1}\cdots P_{\mathrm{M},N_\mathrm{L}}]^T$. In practice, upper and lower limits can be imposed on the elements of $\boldsymbol{P}_\mathrm{M}$ considering the specifications of the LEDs. Hence, it is assumed that $\boldsymbol{P}_\mathrm{M}\in\mathcal{P}$, where $\mathcal{P} = [P_{\min,1},P_{\max,1}]\times\cdots\times[P_{\min,N_\mathrm{L}},P_{\max,N_\mathrm{L}}]$. Similarly, let $\boldsymbol{l}_\mathrm{R}\in\mathcal{L}$, 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 $\boldsymbol{P}_\mathrm{M}$ or $\boldsymbol{l}_\mathrm{R}$.

The location of the VLC receiver can be estimated via the ML estimator [18], which is stated as

$$\left(\widehat{\boldsymbol{l}}_\mathrm{R},\widehat{\boldsymbol{P}}_\mathrm{M}\right) = \underset{\boldsymbol{l}_\mathrm{R}\in\mathcal{L},\boldsymbol{P}_\mathrm{M}\in\mathcal{P}}{\arg\max}\; p(\boldsymbol{P}_\mathrm{R}\,|\,\boldsymbol{l}_\mathrm{R},\boldsymbol{P}_\mathrm{M}) \tag{3}$$

In (3), $p(\boldsymbol{P}_\mathrm{R}\,|\,\boldsymbol{l}_\mathrm{R},\boldsymbol{P}_\mathrm{M})$ denotes the likelihood function, which can be calculated from (1) and (2) as follows:

$$p(\boldsymbol{P}_\mathrm{R}\,|\,\boldsymbol{l}_\mathrm{R},\boldsymbol{P}_\mathrm{M}) = \prod_{i=1}^{N_\mathrm{L}}\left(\frac{\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{M},i}R_ph_i(\boldsymbol{l}_\mathrm{R}))^2}{2\sigma_i^2}} + \frac{1-\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{H},i}R_ph_i(\boldsymbol{l}_\mathrm{R}))^2}{2\sigma_i^2}}\right) \tag{4}$$

From (3) and (4), it can be shown, after some manipulation, that the ML estimator for the location of the VLC receiver becomes

$$\widehat{\boldsymbol{l}}_\mathrm{R} = \underset{\boldsymbol{l}_\mathrm{R}\in\mathcal{L}}{\arg\max}\prod_{i=1}^{N_\mathrm{L}}\left(\frac{\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_\mathrm{R})R_ph_i(\boldsymbol{l}_\mathrm{R}))^2}{2\sigma_i^2}} + \frac{1-\gamma_i}{\sqrt{2\pi}\sigma_i}e^{-\frac{(P_{\mathrm{R},i}-P_{\mathrm{H},i}R_ph_i(\boldsymbol{l}_\mathrm{R}))^2}{2\sigma_i^2}}\right) \tag{5}$$

where $\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_\mathrm{R})$ in (5) is given by

$$\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_\mathrm{R}) = \begin{cases} P_{\min,i}, & \text{if } \frac{P_{\mathrm{R},i}}{R_ph_i(\boldsymbol{l}_\mathrm{R})}\le P_{\min,i} \\ P_{\max,i}, & \text{if } \frac{P_{\mathrm{R},i}}{R_ph_i(\boldsymbol{l}_\mathrm{R})}\ge P_{\max,i} \\ \frac{P_{\mathrm{R},i}}{R_ph_i(\boldsymbol{l}_\mathrm{R})}, & \text{otherwise} \end{cases} \tag{6}$$

Hence, the original formulation of the ML estimator in (3), which requires optimization over an $(N_\mathrm{L}+3)$-dimensional space is reduced to a three-dimensional search in (5).

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:

$$P_{\mathrm{R},i}^{(j)} = R_p\,P_{\mathrm{T},i}^{(j)}\,h_i\big(\boldsymbol{l}_\mathrm{R}^{(j)}\big) + \eta_i^{(j)} \tag{7}$$

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 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 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 (7) is modeled in Scenario 1 as

$$P_{\mathrm{T},i}^{(j)} = \begin{cases} P_{\mathrm{M},i}\,, & \text{with probability } \gamma_i \\ P_{\mathrm{H},i}\,, & \text{with probability } 1-\gamma_i \end{cases} \tag{8}$$

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 (7) is modeled as

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

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

Based on the power measurements in (7), 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 (7):

$$\begin{aligned} \mathcal{H}_i &: P_{\mathrm{R},i}^{(j)} = R_p\, P_{\mathrm{H},i}\, h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) + \eta_i^{(j)},\ j=1,\ldots,N_{\mathrm{V}} \\ \mathcal{M}_i &: P_{\mathrm{R},i}^{(j)} = R_p\, P_{\mathrm{M},i}\, h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) + \eta_i^{(j)},\ j=1,\ldots,N_{\mathrm{V}} \end{aligned} \tag{10}$$

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 [18]. The GLRT for the problem in (10) can be stated as

$$\frac{\max\limits_{P_{\mathrm{M},i}\in[P_{\min,i},P_{\max,i}]} \prod\limits_{j=1}^{N_{\mathrm{V}}} \frac{e^{-\frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{M},i} h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}}{\sqrt{2\pi}\sigma_{i,j}}}{\prod\limits_{j=1}^{N_{\mathrm{V}}} \frac{1}{\sqrt{2\pi}\sigma_{i,j}} e^{-\frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{H},i} h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \tau_i \tag{11}$$

where τ_i denotes the threshold, which can be chosen according to the tradeoff between the conditional probabilities of error [18]. 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. The maximization problem in the numerator of (11) yields the following maximizer:

$$\widehat{P}_{\mathrm{M},i} = \begin{cases} P_{\min,i}, & \text{if } g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big) \le P_{\min,i} \\ P_{\max,i}, & \text{if } g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big) \ge P_{\max,i} \\ g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big), & \text{otherwise} \end{cases} \tag{12}$$

where

$$g\big(\{P_{\mathrm{R},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}\big) \triangleq \frac{\sum_{j=1}^{N_{\mathrm{V}}} P_{\mathrm{R},i}^{(j)} h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)/\sigma_{i,j}^2}{R_p \sum_{j=1}^{N_{\mathrm{V}}} \big(h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big)^2/\sigma_{i,j}^2}\,. \tag{13}$$

Then, the GLRT in (11) can be simplified, after some manipulation, as follows:

$$\begin{aligned} &R_p\big(\widehat{P}_{\mathrm{M},i} - P_{\mathrm{H},i}\big) \sum_{j=1}^{N_{\mathrm{V}}} \frac{P_{\mathrm{R},i}^{(j)} h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)}{\sigma_{i,j}^2} \\ &+ 0.5R_p^2\Big(P_{\mathrm{H},i}^2 - \big(\widehat{P}_{\mathrm{M},i}\big)^2\Big) \sum_{j=1}^{N_{\mathrm{V}}} \frac{\big(h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big)^2}{\sigma_{i,j}^2} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \log(\tau_i) \end{aligned} \tag{14}$$

where $\widehat{P}_{\mathrm{M},i}$ is given by (12).

Let $\widehat{D}_i$ denote the decision of the GLRT in (14), i.e., the decision for the ith LED transmitter, where $i \in \{1,\ldots,N_{\mathrm{L}}\}$. When 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 (14) and the power estimates in (12) 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 (14); that is,

$$\widehat{\mathcal{H}} = \{i \in \{1,\ldots,N_{\mathrm{L}}\} \,|\, \widehat{D}_i = \mathcal{H}_i\} \tag{15}$$

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

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

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

and the resulting ML estimator can be derived as

$$\begin{aligned} \widehat{\boldsymbol{l}}_{\mathrm{R}} = \underset{\boldsymbol{l}_{\mathrm{R}}\in\mathcal{L}}{\arg\min} &\sum_{i\in\widehat{\mathcal{H}}} \frac{(P_{\mathrm{R},i} - P_{\mathrm{H},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2} \\ &+ \sum_{i\in\widehat{\mathcal{M}}} \frac{(P_{\mathrm{R},i} - \widehat{P}_{\mathrm{M},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2} \end{aligned} \tag{17}$$

where $\widehat{P}_{\mathrm{M},i}$ is as in (12) for $i \in \widehat{\mathcal{M}}$.

2) Algorithm 1-(b): In this algorithm, the estimates in (12) are still assumed to be perfect but possible errors in the decisions of the GLRTs in (14) are taken into consideration. Specifically, the probability that the ith LED transmitter is malicious is calculated as follows:

$$\widehat{\gamma}_i = \mathrm{P}(\mathcal{M}_i|\widehat{D}_i) = \frac{\gamma_i \mathrm{P}(\widehat{D}_i|\mathcal{M}_i)}{\gamma_i \mathrm{P}(\widehat{D}_i|\mathcal{M}_i) + (1-\gamma_i)\mathrm{P}(\widehat{D}_i|\mathcal{H}_i)} \tag{18}$$

where $\gamma_i = \mathrm{P}(\mathcal{M}_i)$ 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. Then, the ML estimator is obtained as follows:

$$\widehat{\boldsymbol{l}}_{\mathrm{R}} = \underset{\boldsymbol{l}_{\mathrm{R}} \in \mathcal{L}}{\arg\max} \prod_{i=1}^{N_{\mathrm{L}}} \left(\frac{\widehat{\gamma}_i}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{\mathrm{R},i} - \widehat{P}_{\mathrm{M},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} + \frac{1-\widehat{\gamma}_i}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{\mathrm{R},i} - P_{\mathrm{H},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} \right) \tag{19}$$

where $\widehat{\gamma}_i$ is given by (18) and $\widehat{P}_{\mathrm{M},i}$ is as in (12). It should be noted that $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{M}_i)$ and $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{H}_i)$ can be calculated for the GLRT in (14) 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

$$\begin{aligned} \mathcal{H}_i \;:\; & P_{\mathrm{R},i}^{(j)} = R_p \, P_{\mathrm{H},i} \, h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) + \eta_i^{(j)}, \;\; j = 1, \ldots, N_{\mathrm{V}} \\ \mathcal{M}_i \;:\; & P_{\mathrm{R},i}^{(j)} = R_p \, P_{\mathrm{M},i}^{(j)} \, h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) + \eta_i^{(j)}, \;\; j = 1, \ldots, N_{\mathrm{V}} \end{aligned} \tag{20}$$

Then, the GLRT is given by

$$\frac{\underset{\{P_{\mathrm{M},i}^{(j)}\}_{j=1}^{N_{\mathrm{V}}}}{\max} \prod_{j=1}^{N_{\mathrm{V}}} \frac{1}{\sqrt{2\pi}\sigma_{i,j}} e^{-\frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{M},i}^{(j)} h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}}{\prod_{j=1}^{N_{\mathrm{V}}} \frac{1}{\sqrt{2\pi}\sigma_{i,j}} e^{-\frac{\left(P_{\mathrm{R},i}^{(j)} - R_p P_{\mathrm{H},i} h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)\right)^2}{2\sigma_{i,j}^2}}} \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \kappa_i \tag{21}$$

where κ_i denotes the threshold. The maximization problem in the numerator of (21) can be solved in closed form, which leads to the following simplified form of the GLRT after some manipulation:

$$\sum_{j=1}^{N_{\mathrm{V}}} \frac{1}{\sigma_{i,j}^2} \Bigg(R_p P_{\mathrm{R},i}^{(j)} h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big) \big(\widehat{P}_{\mathrm{M},i}^{(j)} - P_{\mathrm{H},i}\big) + 0.5 R_p^2 \big(h_i\big(\boldsymbol{l}_{\mathrm{R}}^{(j)}\big)\big)^2 \Big(P_{\mathrm{H},i}^2 - \big(\widehat{P}_{\mathrm{M},i}^{(j)}\big)^2 \Big) \Bigg) \underset{\mathcal{H}_i}{\overset{\mathcal{M}_i}{\gtrless}} \log(\kappa_i) \tag{22}$$

where

$$\widehat{P}_{\mathrm{M},i}^{(j)} = \begin{cases} P_{\min,i}\,, & \text{if } \frac{P_{\mathrm{R},i}^{(j)}}{R_p h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)} \leq P_{\min,i} \\ P_{\max,i}\,, & \text{if } \frac{P_{\mathrm{R},i}^{(j)}}{R_p h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)} \geq P_{\max,i}\,. \\ \frac{P_{\mathrm{R},i}^{(j)}}{R_p h_i\left(\boldsymbol{l}_{\mathrm{R}}^{(j)}\right)}\,, & \text{otherwise} \end{cases} \tag{23}$$

Let $\widehat{D}_i$ denote the decision of the GLRT in (22) for $i \in \{1, \ldots, N_{\mathrm{L}}\}$. When 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 estimation of $\boldsymbol{l}_{\mathrm{R}}$ can be performed via the following algorithms in Scenario 2:

1) Algorithm 2-(a): In this algorithm, the decisions of the GLRTs in (22) are assumed to be correct and the likelihood function is stated as

$$p(\boldsymbol{P}_{\mathrm{R}} \,|\, \boldsymbol{l}_{\mathrm{R}}, \boldsymbol{P}_{\mathrm{M}}) = \prod_{i \in \widehat{\mathcal{H}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{\mathrm{R},i} - P_{\mathrm{H},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} \times \prod_{i \in \widehat{\mathcal{M}}} \frac{1}{\sqrt{2\pi}\sigma_i} e^{-\frac{(P_{\mathrm{R},i} - P_{\mathrm{M},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2}} \tag{24}$$

where $\widehat{\mathcal{H}}$ and $\widehat{\mathcal{M}}$ are as defined in (15) and (16), respectively, for the GLRTs in (22). Then, the corresponding ML estimator is derived as

$$\widehat{\boldsymbol{l}}_{\mathrm{R}} = \underset{\boldsymbol{l}_{\mathrm{R}}}{\arg\min} \sum_{i \in \widehat{\mathcal{H}}} \frac{(P_{\mathrm{R},i} - P_{\mathrm{H},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2} + \sum_{i \in \widehat{\mathcal{M}}} \frac{(P_{\mathrm{R},i} - \widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_{\mathrm{R}}) R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2}{2\sigma_i^2} \tag{25}$$

where $\widehat{P}_{\mathrm{M},i}(\boldsymbol{l}_{\mathrm{R}})$ is as in (6) for $i \in \widehat{\mathcal{M}}$.

2) Algorithm 2-(b): In this algorithm, possible errors in the decisions of the GLRTs in (22) are considered by updating the probabilities that the LED transmitters can be malicious as in (18). 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 (5) and (6) by replacing γ_i's in (5) with $\widehat{\gamma}_i$'s obtained from (18).

Remark 2: It is noted that the estimates obtained in the training stage for the power levels of the malicious LED transmitters in (23) 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).

V. 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 $N_{\mathrm{L}} = 9$ 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.

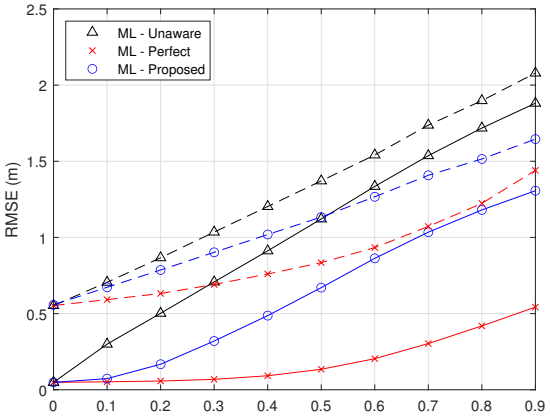

Fig. 1: RMSE versus γ for $\sigma^2 = 10^{-5}$ (dashed lines) and $\sigma^2 = 10^{-6}$ (solid lines).

The orientation vectors, $\boldsymbol{n}_{\mathrm{T}}^i$'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 [19]). Moreover, the orientation of the receiver is specified as $\boldsymbol{n}_{\mathrm{R}} = [0, 0, 1]^T$, i.e., it faces upwards, the area of the PD is taken as $A_{\mathrm{R}} = 1\,\mathrm{cm}^2$, and the responsivity of the PD is set to $R_p = 1$. In the simulations, γ_i's are set to the same value of γ, that is, $\gamma_i = \gamma$ for $i = 1, \ldots, N_{\mathrm{L}}$. Moreover, the noise variances are assumed to be the same, that is, $\sigma_i^2 = \sigma^2$ for $i = 1, \ldots, N_{\mathrm{L}}$. To evaluate the performance of the algorithms, simulations are performed for different levels of noise variances.

To investigate the performance of the proposed ML estimator in (5), the location of the VLC receiver is set to $\boldsymbol{l}_{\mathrm{R}} = [0.5\ 0.5\ 0.85]^T$ meters and various values of γ are considered. For each γ, 10^4 different sets of honest and malicious LED realizations are obtained, and the powers of the malicious LED transmitters, $P_{\mathrm{M},i}$, are generated as uniform random variables over 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 (6), (12), and (23).

In Fig. 1, the RMSE performance of the proposed ML estimator in (5) is plotted versus γ for two different noise levels, namely, $\sigma^2 = 10^{-5}$ (dashed lines) and $\sigma^2 = 10^{-6}$ (solid lines). 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 $P_{\mathrm{T},i} = P_{\mathrm{H},i}$ for $i = 1, \ldots, N_{\mathrm{L}}$, which results in the following ML estimator: $\widehat{\boldsymbol{l}}_{\mathrm{R}} = \underset{\boldsymbol{l}_{\mathrm{R}} \in \mathcal{L}}{\arg\min} \sum_{i=1}^{N_{\mathrm{L}}} (P_{\mathrm{R},i} - P_{\mathrm{H},i} R_p h_i(\boldsymbol{l}_{\mathrm{R}}))^2 / (2\sigma_i^2)$.

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 (25) when $\widehat{\mathcal{H}}$ and $\widehat{\mathcal{M}}$ are equal 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 (5) provides performance improvements (especially for large γ) 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.

To evaluate the performance of the algorithms in Section IV-A, a similar setup is used. The algorithms in this section require a training phase. For this purpose, N_{V} is set to 4 by considering a 2×2 grid of training locations at the following points: $\{(-2, 2, 0.85), (2, 2, 0.85), (2, -2, 0.85), (-2, -2, 0.85)\}$ 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 (14), 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 $\mathrm{P_F}$ for each LED transmitter. In the simulations, two different values of $\mathrm{P_F}$ are considered, namely, $\mathrm{P_F} = 0.01$ and $\mathrm{P_F} = 0.5$. Based on the obtained thresholds, the conditional error and correct decision probabilities, i.e., $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{M}_i)$ and $\mathrm{P}(\widehat{D}_i \,|\, \mathcal{H}_i)$ are calculated using 10^5 Monte-Carlo trials and employed in Algorithm 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. Fig. 2 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 $\mathrm{P_F} = 0.01$, Algorithm 1-(a) has the same performance as the "ML - Unaware" estimator up to $100\,\mathrm{dB}$ 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 $98\,\mathrm{dB}$ but afterwards it achieves lower RMSEs than the case of $\mathrm{P_F} = 0.01$. The main reason for this behavior of Algorithm 1-(a) can be explained as follows: Algorithm 1-(a) estimates the powers of the LED transmitters reasonably well at lower noise variances (see (12)). Even if there exist false alarms, the positioning error can low as power estimates are close to real values. Moreover, it is noted from Fig. 2 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 (18)). 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, 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.

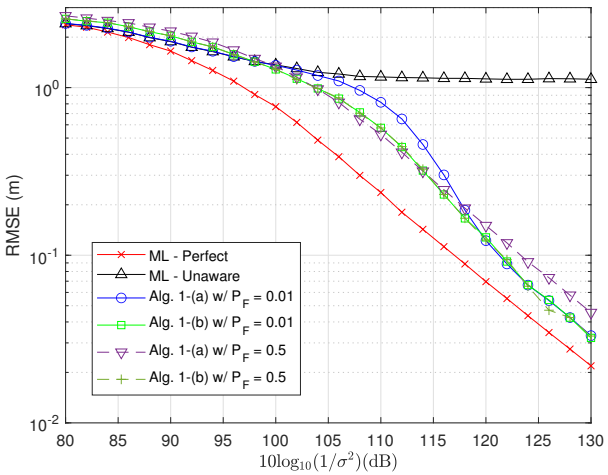

Fig. 2: RMSE versus $10\log_{10}(1/\sigma^2)$ for Scenario 1 ($\gamma = 0.5$).

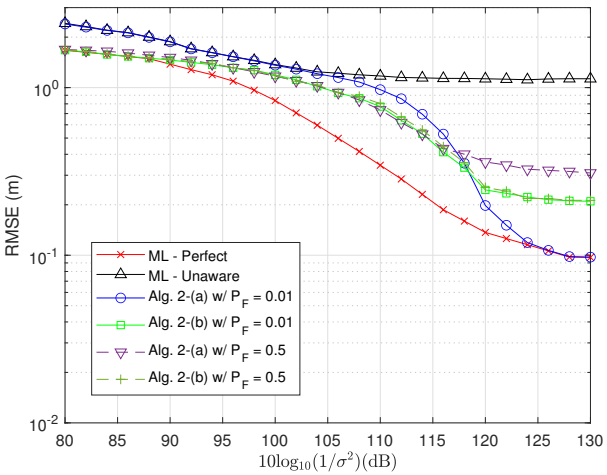

Fig. 3: RMSE versus $10\log_{10}(1/\sigma^2)$ for Scenario 2 ($\gamma = 0.5$).

Again, N_{V} is chosen as 4 by considering the same training points as in the previous case. The training is performed according to the decision rule in (22). To determine κ_i values, the same approach as in Scenario 1 is taken by setting $\mathrm{P_F} = 0.01$ 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. 3 reveal that for $\mathrm{P_F} = 0.01$, 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 $\mathrm{P_F} = 0.5$, it performs closely to "ML - Perfect" at high noise variances but does not converge to "ML - Perfect" at low noise variances. In addition, it is observed that the performance of Algorithm 2-(b) is not affected by the false alarm rate $\mathrm{P_F}$ as in Scenario 1. Thus, Algorithm 2-(b) is robust to changes in κ_i values.

Finally, it is observed 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 higher (lower) noise variances.

VI. Concluding Remarks

Position estimation problems have been formulated for VLP systems in the presence of malicious LED transmitters. 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. As a possible direction for future work, uncertainties in the knowledge of the probabilities that the LED transmitters are malicious (i.e., γ_i's) can be considered.

References

[1] 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.

[2] 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.

[3] 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.

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

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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*, G. S. Buller, R. C. Hollins, R. A. Lamb, M. Laurenzis, A. Camposeo, M. Farsari, L. Persano, and L. E. Busse, Eds., vol. 11540, International Society for Optics and Photonics. SPIE, 2020, pp. 127–137.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

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

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

[19] 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.