Geo-spatial Location Spoofing Detection for Internet of Things

Jing Yang Koh, Ido Nevat, Derek Leong, and Wai-Choong Wong

Abstract—**We develop a new location spoofing detection algorithm for geo-spatial tagging and location-based services in the Internet of Things (IoT), called Enhanced Location Spoofing Detection using Audibility (ELSA). ELSA is based on a statistical decision theory framework and uses Two-Way Time-of-Arrival (TW-TOA) information between the tag and the base-stations. In addition to the TW-TOA information, ELSA exploits the implicitly available audibility information to improve detection rates of location spoofing attacks. Given TW-TOA and audibility information, we derive the decision rule regarding the verification of the user's location, which is based on the Generalised Likelihood Ratio Test. We develop a practical threat model for delay measurements spoofing scenarios, and investigate in detail the performance of ELSA in terms of detection and false alarm rates. Our extensive simulation results on both synthetic and real-data sets demonstrate the superior performances of ELSA compared to conventional non-audibility-aware approaches.**

Index Terms—**Location spoofing detection, Internet of things, Geo-spatial tagging, Audibility, Likelihood Ratio Test, Time of arrival.**

I. Introduction

Wireless localization has been an active research topic in the last decade due to its significance in many existing applications. In particular, the area of detecting *location spoofing* attempts has become increasingly important. This is due to its key role in proliferating applications such as Location-Based Services (LBS) [1], [2], Intelligent Transport Systems (ITS) [3]–[7], Mobile and Ad Hoc Networks (MANET) [5], [8], [9], Wireless Sensor Networks (WSN) [10]–[13], and other mission-critical systems [14], [15]. More recently, the emerging Internet of Things (IoT) technology [16], [17], which require the estimated location of each target device to be accurate became crucial. Without reliable location information, the expected operations and functioning of the applications may be severely disrupted, causing inconvenience to end users or even resulting in the loss of human lives especially in ITS or other applications. In fact, high accuracy and precision are also key requirements in IoT applications [16].

Spatially deployed *anchors* (or reference nodes) can be used to estimate the distance of targets in the range-based Time Of Arrival (TOA) localization techniques [10], [18]–[20]. Specifically, we focus on the TOA-based Two-Way Ranging (TWR) protocol [10], [18]–[20] where a target node simply needs to reply to range request packets sent from the anchors. This enables the anchors to estimate their distances from the target by making use of the time of flight (delay) information. However, a malicious target can attempt to spoof the delay measurements received by the anchors. Therefore, many location spoofing detection schemes [2], [3], [5], [7]–[9], [11], [13], [14], [21], [22] have been proposed to deal with this threat. Typically, the detection system uses the trilateration (or multilateration) method [10], [15], [18] to fuse three or more distance estimates and localize a node in two-dimension [8], [11], [19], [22]. Otherwise, there may exist ambiguity in the location estimates.

However, we show that this fundamental assumption can be relaxed to just two *audible* anchors. In contrast to prior works which simply ignore inaudible anchors (i.e., the inaudible anchors are completely excluded by the trilateration method), we exploit the implicitly available *outage* (or inaudibility) information to improve the location spoofing detection rate at essentially no additional cost. Utilizing the concept of audibility, we develop a Generalized Likelihood Ratio Test (GLRT) [23] called ELSA to detect location spoofing attacks. The statistical GLRT hypothesis testing technique is a well-recognized approach that can be used to distinguish the received TOA delay measurements from an honest or malicious target. We choose TOA-based localization as it is widely used (e.g., in Global Positioning System (GPS)) and provides the best accuracy (e.g., in the range of centimeters for Ultra-Wide Band (UWB) devices [18], [24], [25]) compared to other range-based (e.g., Received Signal Strength (RSS)) and range-free approaches [26]. We consider GPS-denied indoor or urban environments where the GPS measurements are not readily available [19]. We then study the effectiveness of ELSA under adversarial settings and show that it significantly outperforms the conventional non-audibility-aware TOA-based approaches (e.g., [4] adopted a similar likelihood ratio test approach, but had not considered audibility in its likelihood probability functions).

Unlike typical wireless network deployments, the anchors in an IoT environment are typically off-the-shelf low cost tags due to their scalability. As such, these limited capability tags do not output any RSS readings (see e.g., [27], [28]). Despite this, our approach is well suited for these scenarios as it derives the implicit audibility information from the received delay measurements. At the same time, our approach is also compatible with existing infrastructure-based TOA ranging schemes and does not require additional cryptographic operations or message exchanges between the anchors and the target. To the best of our knowledge, this is the first attempt to incorporate audibility information for location spoofing detection. Next, we briefly review existing works in the literature. The target and anchor are also known as the prover and verifier respectively in location verification schemes. The work in [1] presented a framework for using witness nodes to validate the location of targets. Specifically, the witnesses use a cryptographic asserted location proof protocol to verify their distances to the target. Next, [8] presented a similar, but distributed cooperative witnesses protocol to verify location claims through a series of message exchanges. Likewise, [13] proposed a method to check if the target lies within a claimed region and whether the claimed location exceeds a reasonable bound. Anonymous beacons were used in [7] to verify a target location. [11] further assumed the existence of hidden and mobile anchors to verify the location of nodes via distance bounding protocols [21]. [22] modeled the location verification problem as a non-cooperative two-player game between the anchors and the malicious target to compute the best placement for the anchors.

Different from the above works which rely extensively on extra message exchange protocols, cryptography or special assumptions, the works in [2]–[5] used the information theoretic Likelihood Ratio Test (LRT) approach to verify the location of targets via the RSS-based localization method. Clearly, such statistical approaches are advantageous in practical scenarios as they can tolerate naturally occurring observation noise which can otherwise trigger false alarms. Thus, we adopt a similar statistical approach and devise a LRT to detect location spoofing attacks. Different from the typical location verification schemes which are used to verify a claimed location, we tackle the challenging scenario where the anchors themselves localize a target and verify that it is not spoofing its location.

The key contributions of this paper can be summarized as follows:

- We introduce the notion of *audibility* and develop a framework for utilizing it to detect location spoofing attempts.
- We design ELSA, an audibility-aware GLRT test to detect location spoofing attempts and prove that it has better detection rates than the conventional non-audibility-aware GLRT test.
- We verify the efficacy of ELSA using both extensive simulations and a real-life experimental dataset.

The rest of this paper is organized as follows. Section II presents a motivating example for our proposed framework. Section III introduces the model and the problem formulation is given in Section IV. Section V presents our experimental results and discussion. Finally, conclusions are drawn in Section VII.

We use the following notations in the paper. Upper-case letters denote random variables and the corresponding lower-case letters their realizations. Bold letters represent vectors, while $\mathcal{N}(x;\mu,\sigma^2)$ represents the normal pdf, which is defined as $\mathcal{N}(x;\mu,\sigma^2)=\frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$, and $\Phi(.)$ is the normal cdf, which is defined as $\Phi(x)=\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x}e^{-\frac{t^2}{2}}dt$, and we let $p(x)=P(\mathrm{X}=x)$. Finally, we use $\mathbb{1}(\cdot)$ to denote the indicator function which equals one if its function argument $(\cdot)$ is true and zero otherwise.

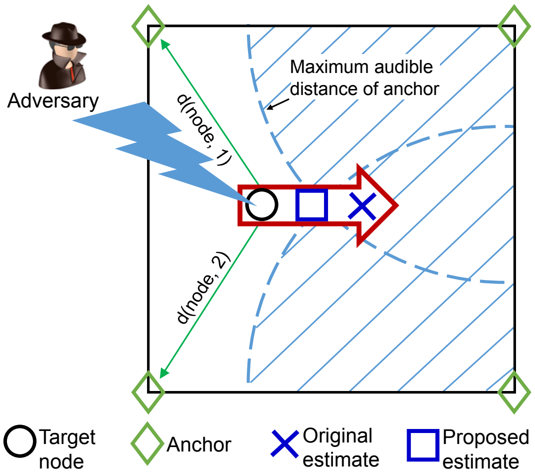


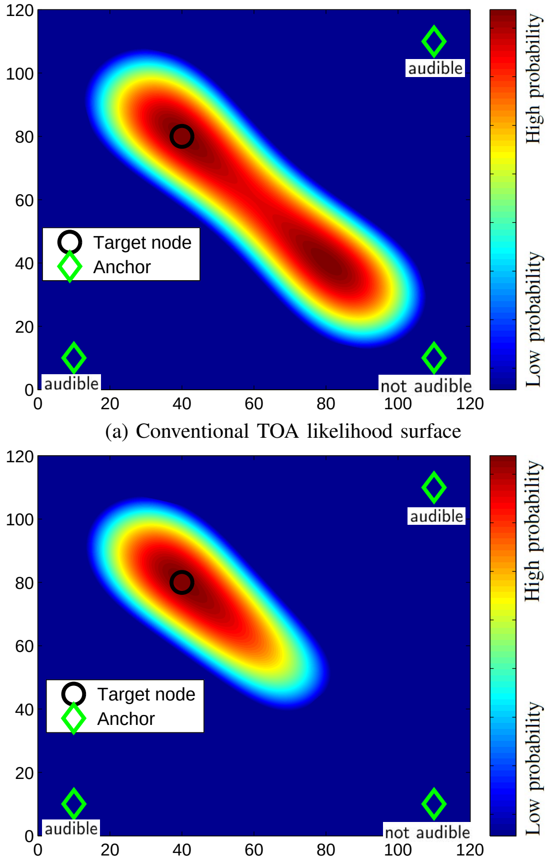
Fig. 1: Illustration of proposed method where a malicious target node attempts to spoof its location by adding delays to the delay measurements $d(\text{node},\text{anchor})$.

II. Motivating Example For Proposed Audibility Framework

We first illustrate with an example of the location spoofing attack and how audibility aids in detecting the attacks. Shown in Fig. 1 is a room with an anchor at each corner. Suppose that a malicious target node at the left side of the room (denoted by the circle) is in the audible range of two anchors and wishes to spoof its location to appear at the other side of the room (marked with a cross). If the target is controlled by an adversary, it can add additional delays to increase its TOA delay measurement [6], [9], [15], [21], [22], [29], [30] and hence increase the estimated distance from itself to the two anchors. Otherwise, an external adversary may also selectively jam the wireless channel to introduce delays [31]–[33]. The threat model will be detailed in Section III-D. Using the conventional approaches, a detection system will not be able to detect the location spoofing attempt as there are insufficient contradictory information to raise suspicions. However, using the additional implicitly available audibility information as input, it is now unlikely that the target is located at the cross since it is not in the range of the two anchors at the right side of the room. The target is most likely to be located around the square shown in Fig. 1. (Note that in actual scenarios, the location estimates may be a small region of equally likely points (see Fig. 2) instead of an exact location point as shown above, but the concept remains the same.) Hence, we can detect the location spoofing attack by comparing the likelihood probabilities.

A. How Audibility Aids in Location Spoofing Detection

Using the conventional trilateration technique [10], [15], [18] (without utilizing audibility information), distance estimates from at least three different non-collinear anchors are needed to localize a target node. Otherwise, there may exist ambiguity when there are only two delay measurements. For example, the target node may be equally likely to be at two separate regions as seen from the target's likelihood heat map in Fig. 2a. However, this ambiguity can be significantly



(a) Conventional TOA likelihood surface

(b) TOA likelihood surface with audibility information

Fig. 2: Log-likelihood heat map for the location of a target node with three anchors (of which two are audible). Regions with higher probabilities for the target's location are represented by lighter colors.

reduced once we incorporate the audibility information (see Fig. 2b). As a result, the bottom right region is now unlikely since there exists a nearby anchor that does not receive any delay measurement (not audible). Therefore, by taking advantage of the "missing delay measurements" or the inaudibility information, we are able to relax the fundamental three distance estimates assumption without using any additional hardware or message exchanges. This leads to an improved accuracy of the TOA localization algorithm at no extra cost. The audibility information can be exploited because the missing observations are *Missing Not At Random (MNAR)* as termed by Rubin in his seminal work [34] where he developed a statistical framework to account for missing data. Thus, we should not ignore the missing delay observations as it provides additional information about the target location.

III. Network Model

In this section, we introduce the definitions for audibility and describe our system and threat models for the location spoofing detection system which uses the TOA-based Two-Way Ranging (TWR) protocol.

A. Connectivity Model

In order for two nodes A and B to communicate with each other, the transmitted signals should be audible to the other party. This is modeled as the widely used power loss model [35].

Definition 1 (Power loss model)**.** *The received signal power by a node A located at $\mathbf{\Theta}_A = \left[x^{(A)} \;\; y^{(A)}\right]$ from a signal sent by node B which is located at $\mathbf{\Theta}_B = \left[x^{(B)} \;\; y^{(B)}\right]$ is given by*

$$P_R = P_T - 10\alpha \log \frac{d\left(A,B\right)}{d_0} + \epsilon,$$

where P_T is the transmitted power by node B, α is the path-loss exponent, $d\left(A,B\right) := \sqrt{\left(x^{(A)} - x^{(B)}\right)^2 + \left(y^{(A)} - y^{(B)}\right)^2}$ is the Euclidean distance between nodes A and B, d_0 is a reference distance and $\epsilon \sim \mathcal{N}\left(0, \sigma_\epsilon^2\right)$ represents the shadowing effect.

If node B is able to receive signals transmitted by node A, then the former is said to be to be audible. More formally, we define audibility as the following.

Definition 2 (Audibility)**.** *Node B is said to be audible to node A if*

$$P_R = P_T - 10\alpha \log \frac{d\left(A,B\right)}{d_0} + \epsilon \geq \lambda,$$

where λ is a pre-defined threshold representing the receiver's sensitivity.

B. Two-Way Ranging (TWR) Distance Estimation Protocol

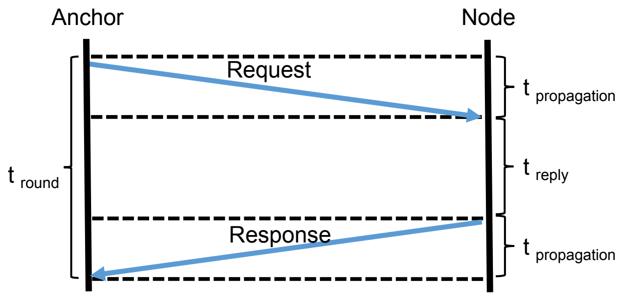


Fig. 3: Message exchange of the TWR protocol [36].

The TWR protocol is a time of arrival (TOA)/flight (TOF) based ranging method specified in the IEEE 802.15.4a standard [36]. It is gaining popularity especially in small low-cost UWB devices. It allows two communicating devices to estimate their distance from each other without needing time synchronization. First, the anchor sends a range request packet to an unlocalized target node. The latter then waits for some known time t_{reply} before sending a response packet back to the anchor. The value of t_{reply} is assumed to be known to both devices. Assuming that there are no measurement errors, the anchor is able to obtain the round trip time of the two packets t_{round} by subtracting the time it first sent a request packet from the time it received the response packet. Since

$$t_{\text{round}} = 2 \times t_{\text{propagation}} + t_{\text{reply}},$$

the value of the packet propagation *delay* or $t_{\text{propagation}} = \frac{t_{\text{round}} - t_{\text{reply}}}{2}$ can be determined and subsequently the distance between the node and the anchor can be computed as follows:

$$d(\text{node}, \text{anchor}) = t_{\text{propagation}} \times v_p$$

where v_p is the signal propagation speed. No time synchronization between the two nodes is required in the TWR protocol as the anchor node uses its own local clock information to infer distance. This advantage enables the protocol to be used even with low cost RFID tags where time synchronization is not possible [37]. With sufficient range-based distance estimates, a node can be localized using the trilateration or multilateration techniques [10], [15], [18].

C. System Model

We consider a scenario where a fusion center receives some delay measurements from its anchors (also known as reference nodes) and fuses the measurements to verify a target node's location. We present the considered wireless system with the following assumptions:

1) Assume a wireless network with n static anchors where the location of the i^{th} anchor (verifier) is denoted by

$$\mathbf{x}_i = [x_i \ y_i],$$

where its 2D coordinates $x_i, y_i \in \mathbb{R}$ for $i \in \{1, \ldots, n\}$.

2) The true location of the target node (prover) is denoted by

$$\boldsymbol{\Theta} = [x_\theta \ y_\theta],$$

where its 2D coordinates $x_\theta, y_\theta \in \mathbb{R}$. Depending on the deployment scenario, we assume that there is a prior $p(\boldsymbol{\Theta})$ for the target node. A uniform prior can be assigned if the target is equally likely to exist anywhere in the considered region.

3) We consider a scenario where the TWR protocol [36] is used. Each anchor i in the communication range of the target node will receive a delay measurement [10] which can be represented by:

$$t_i = \frac{d(\boldsymbol{\Theta}, \mathbf{x}_i)}{v_p} + W_i, \qquad (1)$$

where $d(\mathbf{a}, \mathbf{b})$ is the Euclidean distance between two locations $\mathbf{a}, \mathbf{b}$ and is given by

$$d(\mathbf{a}, \mathbf{b}) = \sqrt{(a_x - b_x)^2 + (a_y - b_y)^2}, \qquad (2)$$

v_p is the signal propagation speed and W_i is the time delay error assumed to be an i.i.d. Gaussian random variable given by $W_i \sim \mathcal{N}(0, \sigma_W^2)$[1].

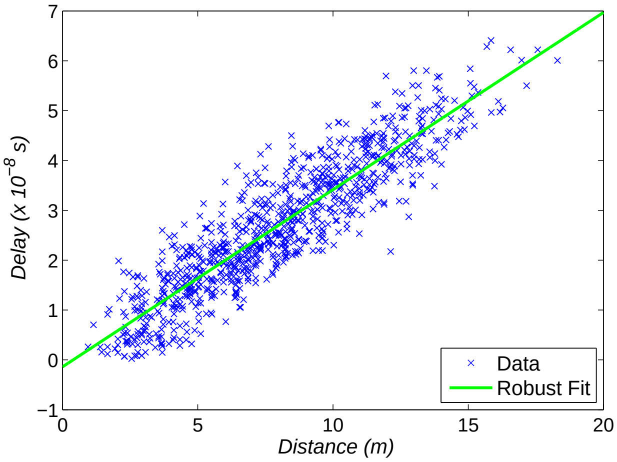


Fig. 4: TOA delay as a function of distance.

4) In our audibility model, each anchor i in the communication range of the target node will receive a signal with a received power P_i (or received signal strength (RSS)) that is equal or higher than the minimum signal receiving threshold λ. We use the widely accepted log-normal propagation model [10] to estimate the received power of the signal:

$$P_i = P_t - 10\alpha \log \frac{d(\boldsymbol{\Theta}, \mathbf{x}_i)}{d_0} + \epsilon_i \geq \lambda \qquad (3)$$

where P_t is the received power from the transmitter at a reference distance d_0 (typically 1 meter), α is the path loss exponent, and ϵ_i is the received power error assumed to be an i.i.d. Gaussian random variable given by $\epsilon_i \sim \mathcal{N}(0, \sigma_\epsilon^2)$.

5) If an anchor i does not receive any signal from the target node, we can treat the received signal as having a received power P_i that is less than the minimum signal receiving threshold λ. i.e., $P_i < \lambda$.

6) We let r_i be an indicator variable that depends on whether the anchor i receives a delay measurement from the target node (see Eq. (3)):

$$r_i = \begin{cases} 1 & \text{if } P_i \geq \lambda, \\ 0 & \text{otherwise.} \end{cases} \qquad (4)$$

Empirical Support for Chosen TOA and RSS Models

Our chosen TOA and RSS models in Eq. (1) and Eq. (3) respectively are supported by the experimental measurements obtained from [38]. The TOA and RSS measurements are plotted in Figs. 4 and 5 respectively. As seen from the figures, the zero mean Gaussian noise and linearity assumptions are reasonable and provide good representation of the actual data. A Kolmogorov-Smirov (KS) test was also used in [38] which showed that the Gaussian assumption is valid under a 0.05 significance level.

D. Threat Model

We consider an adversary who wants to significantly perturb a target's perceived location by the fusion center $\widehat{\boldsymbol{\Theta}}$ from its true location $\boldsymbol{\Theta}$. This can be achieved by **manipulating the delay measurements** received by the anchors as discussed in our motivating example in Section II. Recall that a non-tampered delay measurement received at the i^{th} anchor is given by:

$$t_i = \frac{d(\boldsymbol{\Theta}, x_i)}{v_p} + W_i.$$

[1] Note that W_i may also be replaced by any known parametric distribution.

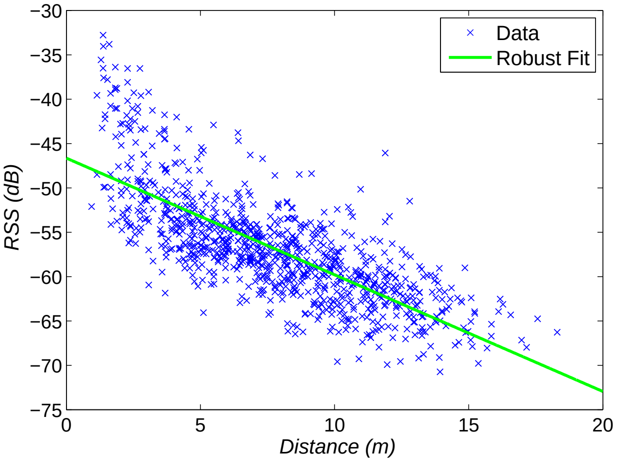


Fig. 5: RSS value as a function of distance.

The malicious target (in the case of an *internal* adversary) can falsify its location by adding a delay δ_i before replying a TWR request message such that the received delay measurement becomes:

$$t_i = \frac{d(\boldsymbol{\Theta}, x_i)}{v_p} + W_i + \delta_i \tag{5}$$

where we assume $\delta_i \overset{i.i.d.}{\sim} \mathcal{N}(\mu_\delta, \sigma_\delta^2)$. The Gaussian model is used for analytical convenience. In practice, only a positive delay may be added. The latter is known as the distance enlargement attack in the literature [6], [9], [15], [21], [22], [29], [30]. Since the distance estimate computed by an anchor i is equivalent to

$$\begin{aligned}\widehat{d}(\boldsymbol{\Theta}, X_i) &= t_i v_p \\ &= \left(\frac{d(\boldsymbol{\Theta}, X_i)}{v_p} + W + \delta_i\right) v_p,\end{aligned} \tag{6}$$

where $v_p >> 0$, a small value of delay δ_i (e.g., 10^{-9}) is sufficient to cause a large difference in the estimated distance (approximately 30cm, in the case of radio waves).

An *external* adversary may also increase the delay measurement by some δ through the exploitation of the underlying medium access control (MAC) protocol or via signaling attacks [31]–[33]. For example, wireless devices using the ALOHA and carrier sense multiple access with collision avoidance (CSMA/CA) protocols [20], [39] are vulnerable to increased transmission delays during high traffic loads. Hence, an adversary can increase the delay measurement of a target by generating radio interference to decrease the signal-to-noise ratio (SNR) [10], [12], [24] of legitimate signals or by transmitting many packets to cause congestion [40]. We do not address the authentication issue in this paper and assume that the targets are able to authenticate themselves to the fusion center if necessary.

IV. ELSA: Enhanced Location Spoofing Detection using Audibility

We present the *location spoofing* detection algorithm ELSA which utilizes both TOA measurements and the implicit *audibility* information to verify that a target is not spoofing its delay measurements.

A. Problem Formulation: Optimal Detection

In order to achieve this task, a common approach would be to construct a binary hypothesis test to verify the received delay measurements. The well-known Likelihood Ratio Test (LRT) which is the optimal test (justified by the Neyman-Pearson lemma [23], [41]) can be used to detect location spoofing attempts under the two competing hypotheses:

$$\begin{aligned}&\mathcal{H}_0 : \text{no location spoofing}\\ &\mathcal{H}_1 : \text{location spoofing attempt.}\end{aligned} \tag{7}$$

The LRT[2] can be formulated as:

$$\Lambda(\mathbf{t}, \mathbf{r}) \triangleq \frac{p(\mathbf{t}, \mathbf{r}|\mathcal{H}_1)}{p(\mathbf{t}, \mathbf{r}|\mathcal{H}_0)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta, \tag{8}$$

where the bold letters $\mathbf{t}$ and $\mathbf{r}$ represent vectors of delay observations $\mathbf{t} = [t_1, \ldots, t_n]$ and audibility indicator values $\mathbf{r} = [r_1, \ldots, r_n]$ from the n anchors respectively, and η is a chosen threshold.

Under the Neyman-Pearson lemma, the LRT is the most powerful test at each significance level α (false alarm) for a threshold η where $p(\Lambda(\mathbf{t}, \mathbf{r}) > \eta|\mathcal{H}_0) = \alpha$. The functions $p(\mathbf{t}, \mathbf{r}|\mathcal{H}_0)$ and $p(\mathbf{t}, \mathbf{r}|\mathcal{H}_1)$ represent the likelihood functions for the null hypothesis and alternative hypothesis respectively. Since we treat $\boldsymbol{\Theta}$ as an unknown random variable, the likelihood functions can be formulated as

$$\begin{aligned}p(\mathbf{t}, \mathbf{r}|\mathcal{H}_j) &= \int p(\mathbf{t}, \mathbf{r}|\boldsymbol{\Theta}, \mathcal{H}_j) p(\boldsymbol{\Theta}|\mathcal{H}_j)\, d\boldsymbol{\Theta}\\ &= \int p(\mathbf{t}|\mathbf{r}, \boldsymbol{\Theta}, \mathcal{H}_j) p(\mathbf{r}|\boldsymbol{\Theta}, \mathcal{H}_j) p(\boldsymbol{\Theta}|\mathcal{H}_j)\, d\boldsymbol{\Theta}.\end{aligned}$$

However, a closed form expression to the above integral is intractable due to the non-linear relationship in $p(\mathbf{t}, \mathbf{r}|\boldsymbol{\Theta}, \mathcal{H}_j)$. Hence, the LRT in Eq. (8) is no longer applicable. Instead, it is common to use the Generalized Likelihood Ratio Test (GLRT) [23], [41]), given by

$$\Lambda(\mathbf{t}, \mathbf{r}) \triangleq \frac{p(\mathbf{t}, \mathbf{r}|\mathcal{H}_1, \widehat{\boldsymbol{\Theta}}_{\text{MAP}}^{\mathcal{H}_1})}{p(\mathbf{t}, \mathbf{r}|\mathcal{H}_0, \widehat{\boldsymbol{\Theta}}_{\text{MAP}}^{\mathcal{H}_0})} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta, \tag{9}$$

where we approximate $p(\mathbf{t}, \mathbf{r}|\mathcal{H}_j)$ using the maximum-a-posteriori (MAP) estimate $\widehat{\boldsymbol{\Theta}}_{\text{MAP}}^{\mathcal{H}_j}$. We now derive the MAP estimate $\widehat{\boldsymbol{\Theta}}_{\text{MAP}}^{\mathcal{H}_j}$.

[2] The LRT for the conventional non-audibility-aware approach (See Appendix A) is $\Lambda(\mathbf{t}) \triangleq \frac{p(\mathbf{t}|\mathcal{H}_1)}{p(\mathbf{t}|\mathcal{H}_0)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta$.

B. Derivation of MAP Estimate

The MAP estimate is given by

$$\begin{aligned}\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}} &= \arg\max_{\mathbf{\Theta}} p(\mathbf{\Theta}|\mathbf{t},\mathbf{r},\mathcal{H}_j)\\ &= \arg\max_{\mathbf{\Theta}} p(\mathbf{t},\mathbf{r}|\mathbf{\Theta},\mathcal{H}_j)p(\mathbf{\Theta}|\mathcal{H}_j)\\ &= \arg\max_{\mathbf{\Theta}} p(\mathbf{t}|\mathbf{r},\mathbf{\Theta},\mathcal{H}_j)P(\mathbf{r}|\mathbf{\Theta},\mathcal{H}_j)p(\mathbf{\Theta}|\mathcal{H}_j)\\ &= \arg\max_{\mathbf{\Theta}} \prod_{i=1}^{n}\Big[p(t_i|r_i,\mathbf{\Theta},\mathcal{H}_j)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0)\Big]\\ &\quad\times P(r_i|\mathbf{\Theta},\mathcal{H}_j)p(\mathbf{\Theta}|\mathcal{H}_j)\\ &= \arg\max_{\mathbf{\Theta}} \sum_{i=1}^{n}\Big[\log p(t_i|r_i,\mathbf{\Theta},\mathcal{H}_j)\mathbb{1}(r_i=1)\\ &\quad+\log P(r_i|\mathbf{\Theta},\mathcal{H}_j)\Big]+\log p(\mathbf{\Theta}|\mathcal{H}_j)\\ &= \arg\max_{\mathbf{\Theta}} \sum_{i=1}^{n}\log\mathcal{N}(t_i;\frac{d(\mathbf{\Theta},\mathbf{x}_i)}{v_p}+\delta_i,\sigma_W^2)\mathbb{1}(r_i=1)\\ &\quad+\sum_{i=1}^{n}\log P(r_i=1|\mathbf{\Theta},\mathcal{H}_j)\mathbb{1}(r_i=1)\\ &\quad+P(r_i=0|\mathbf{\Theta},\mathcal{H}_j)\mathbb{1}(r_i=0)+\log p(\mathbf{\Theta}|\mathcal{H}_j).\end{aligned}\tag{10}$$

The indicator function $\mathbb{1}(\cdot)$ is used to ensure that the product is non-zero when no delay measurements are received. The probability of anchor i observing a delay measurement t_i is given by:

$$P(t_i|r_i,\mathbf{\Theta})=\mathcal{N}(t_i;\frac{d(\mathbf{\Theta},\mathbf{x}_i)}{v_p}+\delta_i,\sigma_W^2)\mathbb{1}(r_i=1),$$

and the probability of anchor i receiving a signal with a RSS value that is greater or equal to the minimum signal receiving threshold λ is given by:

$$\begin{aligned}P(r_i=1|\mathbf{\Theta}) &= \int_{\lambda}^{\infty}\mathcal{N}(r_i;P_t-10\alpha\log\frac{d(\mathbf{\Theta},\mathbf{x}_i)}{d_0},\sigma_\epsilon^2)\,dr_i\\ &= 1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\frac{d(\mathbf{\Theta},\mathbf{x}_i)}{d_0}}{\sigma_\epsilon}\right).\end{aligned}$$

On the other hand, we can compute the probability that the anchor i does not receive a delay measurement which is given by

$$\begin{aligned}P(r_i=0|\mathbf{\Theta}) &= \int_{-\infty}^{\lambda}\mathcal{N}(r_i;P_t-10\alpha\log\frac{d(\mathbf{\Theta},\mathbf{x}_i)}{d_0},\sigma_\epsilon^2)\,dr_i\\ &= \Phi\left(\frac{\lambda-P_t+10\alpha\log\frac{d(\mathbf{\Theta},\mathbf{x}_i)}{d_0}}{\sigma_\epsilon}\right).\end{aligned}$$

Therefore, the generalized likelihood function can be expressed as:

$$\begin{aligned}&p(\mathbf{t},\mathbf{r}|\mathcal{H}_j,\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}})=p(\mathbf{t}|\mathbf{r},\mathcal{H}_j,\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}})p(\mathbf{r}|\mathcal{H}_j,\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}})\\ &=\prod_{i=1}^{n}\left[\mathcal{N}(t_i;\frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}},\mathbf{x}_i)}{v_p},\sigma_W^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0)\right]\\ &\quad\times\prod_{i=1}^{n}\left[p(r_i=1|\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}})\mathbb{1}(r_i=1)+p(r_i=0|\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}})\mathbb{1}(r_i=0)\right]\\ &=\prod_{i=1}^{n}\left[\mathcal{N}(t_i;\frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}},\mathbf{x}_i)}{v_p},\sigma_W^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0)\right]\\ &\quad\times\prod_{i=1}^{n}\left[1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}},\mathbf{x}_i)}{d_0}}{\sigma_\epsilon}\right)\right]\mathbb{1}(r_i=1)\\ &\quad+\Phi\left(\frac{\lambda-P_t+10\alpha\log\frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_j}_{\mathrm{MAP}},\mathbf{x}_i)}{d_0}}{\sigma_\epsilon}\right)\mathbb{1}(r_i=0).\end{aligned}$$

C. Derivation of Test Statistic

Under the null hypothesis $\mathcal{H}_0$, the likelihood function is simply

$$p(\mathbf{t},\mathbf{r}|\mathcal{H}_0,\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}})=p(\mathbf{t}|\mathbf{r},\mathcal{H}_0,\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}})p(\mathbf{r}|\mathcal{H}_0,\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}}),\tag{11}$$

where

$$\begin{aligned}&p(\mathbf{t}|\mathbf{r},\mathcal{H}_0,\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}})\\ &\quad=\prod_{i=1}^{n}\Big[\mathcal{N}(t_i;\frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}},\mathbf{x}_i)}{v_p},\sigma_W^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0)\Big],\end{aligned}$$

and

$$\begin{aligned}&p(\mathbf{r}|\mathcal{H}_0,\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}})=\\ &\prod_{i=1}^{n}\Big[P(r_i=1|\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}})\mathbb{1}(r_i=1)+P(r_i=0|\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}})\mathbb{1}(r_i=0)\Big].\end{aligned}$$

Under the alternative hypothesis $\mathcal{H}_1$,

$$p(\mathbf{t},\mathbf{r}|\mathcal{H}_1,\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}})=p(\mathbf{t}|\mathbf{r},\mathcal{H}_1,\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}})p(\mathbf{r}|\mathcal{H}_1,\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}}),\tag{12}$$

where

$$\begin{aligned}&p(\mathbf{t}|\mathbf{r},\mathcal{H}_1,\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}})=\\ &\prod_{i=1}^{n}\Big[\mathcal{N}(t_i;\frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}},\mathbf{x}_i)}{v_p}+\mu_\delta,\sigma_W^2+\sigma_\delta^2)\mathbb{1}(r_i=1)+\mathbb{1}(r_i=0)\Big],\end{aligned}$$

and

$$\begin{aligned}&p(\mathbf{r}|\mathcal{H}_1,\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}})=\\ &\prod_{i=1}^{n}\Big[P(r_i=1|\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}})\mathbb{1}(r_i=1)+P(r_i=0|\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}})\mathbb{1}(r_i=0)\Big].\end{aligned}$$

Substitution of the values obtain from Eq. (11) and Eq. (12) into Eq. (9) will give the test statistic:

$$\Lambda(\mathbf{t},\mathbf{r}) =$$
$$\prod_{i=1}^{n}\left[\mathcal{N}(t_i; \frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\text{MAP}},\mathbf{x}_i)}{v_p} + \mu_\delta, \sigma_W^2 + \sigma_\delta^2)\mathbb{1}(r_i = 1) + \mathbb{1}(r_i = 0)\right]$$
$$\times \prod_{i=1}^{n}\left[P(r_i = 1|\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\text{MAP}})\mathbb{1}(r_i = 1) + P(r_i = 0|\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\text{MAP}})\mathbb{1}(r_i = 0)\right]$$
$$\div \left[\prod_{i=1}^{n}\mathcal{N}(t_i; \frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\text{MAP}},\mathbf{x}_i)}{v_p}, \sigma_W^2)\mathbb{1}(r_i = 1) + \mathbb{1}(r_i = 0)\right]$$
$$\times \left[P(r_i = 1|\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\text{MAP}})\mathbb{1}(r_i = 1) + P(r_i = 0|\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\text{MAP}})\mathbb{1}(r_i = 0)\right]$$
$$\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta. \tag{13}$$

The following algorithm summaries the steps in the proposed ELSA.

Algorithm 1: ELSA's algorithm for detecting location spoofing attempts.

```
function ELSA($t_{1,\ldots,n}, x_{1,\ldots,n}, \eta, v_p, d_0, P_t, \lambda, \mu_\delta, \alpha, \sigma_W^2, \sigma_\epsilon^2, \sigma_\delta^2$);

Input  : Delay measurements received from the target $t_{1,\ldots,n}$,
         positions of the anchors $x_{1,\ldots,n}$, threshold $\eta$, and the
         system parameters.
Output: Binary result of hypothesis test.
Compute MAP estimate for $\mathcal{H}_0$ (no location spoofing), $\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\text{MAP}}$
  via Eq. (10) (with $\delta_i = 0$).
Compute MAP estimate for $\mathcal{H}_1$ (location spoofing attempt),
  $\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\text{MAP}}$ via Eq. (10) (with $\delta_i \neq 0$).
Compute likelihood probabilities for the two MAP estimates,
  $p(\mathbf{t},\mathbf{r}|\mathcal{H}_0,\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\text{MAP}})$ and $p(\mathbf{t},\mathbf{r}|\mathcal{H}_1,\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\text{MAP}})$ via Eq. (11) and
  Eq. (12) respectively.
Compute the decision rule $\Lambda(\mathbf{t},\mathbf{r}) = \frac{p(\mathbf{t},\mathbf{r}|\mathcal{H}_1,\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\text{MAP}})}{p(\mathbf{t},\mathbf{r}|\mathcal{H}_0,\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\text{MAP}})}$ via
  Eq. (13).
Reject $\mathcal{H}_0$ (no location spoofing) if $\Lambda(\mathbf{t},\mathbf{r}) > \eta$. Otherwise,
  accept $\mathcal{H}_1$ (location spoofing detected).
```

Next, we prove using the following theorem that ELSA provides better detection rates than the conventional non-audibility-aware GLRT test for the same false alarm rate tradeoff.

Theorem 1. *For a fixed false alarm rate, the proposed audibility-aware GLRT test will have a detection rate P_d^{A} that is higher than the conventional GLRT test P_d^{NA} which does not take into account audibility. i.e.,*

$$P_d^{\text{A}} \geq P_d^{\text{NA}}.$$

Proof. See Appendix B. □

V. Experimental Results and Discussion

In this section, we evaluate the performance of the proposed ELSA against the conventional (labeled as 'original' in the figures) GLRT test which does not take into account audibility (similar to the work in [4]) in terms of the location spoofing detection rate. Both simulations and data from a real-life dataset (available in [42]) were used in our evaluation. The MATLAB code used to obtain the simulation results is available as supplemental material, which can be found at [43]. Unless otherwise stated, the following parameters were used in our simulations.

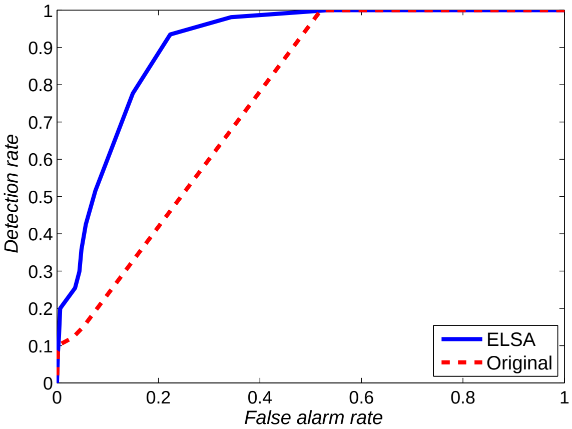


Fig. 6: ROC curves for 3 anchors (of which 2 are audible).

TABLE I: Simulation parameters.

parameter	value (unit)	distance
TOA noise σ_W	10^{-8}s	3m
RSS noise σ_ϵ	$\sqrt{10}$ dBm	
attacker's delay mean, μ_δ	4×10^{-8}s	12m
attacker's delay s.d. σ_δ	4×10^{-8}s	12m
path loss exponent, α	3.2	
transmit power, P_t at $d_0 = 1$m	-40 dBm	
signal receiving threshold, λ	-102 dBm	

A. *Simulation Results for Synthetic Data*

First, we study the effects of utilizing the audibility information using simulations. We consider the scenario where there exist three anchors at the corners of a $100\text{m} \times 100\text{m}$ area as shown in Fig. 2 and the target node is selected uniformly at random inside this area (hence, $p(\mathbf{\Theta}) = \text{unif}(0, 100) \times \text{unif}(0, 100)$). We used a grid search with a one meter granularity to search for the optimal target location using the MAP approach (see Eq. (10)). A finer granularity would improve the accuracy of the schemes, but the improvement would not be significant. Under an adversarial environment, the received delay measurements are adjusted accordingly as discussed in our threat model in Section III-D.

1) ROC Curve Performance: We use the Receiver Operating Characteristic (ROC) curve to compare the detection and false alarm performances of our proposed detection test, ELSA, against the conventional non-audibility-aware GLRT test. For a given decision rule η, the detection rate is given by

$$P(\Lambda(\mathbf{t},\mathbf{r}) > \eta|\mathcal{H}_1),$$

and the false alarm rate is given by

$$P(\Lambda(\mathbf{t},\mathbf{r}) > \eta|\mathcal{H}_0).$$

In Fig. 6, we plot the ROC curves for scenarios when an attacker adds a positive delay to the delay measurements

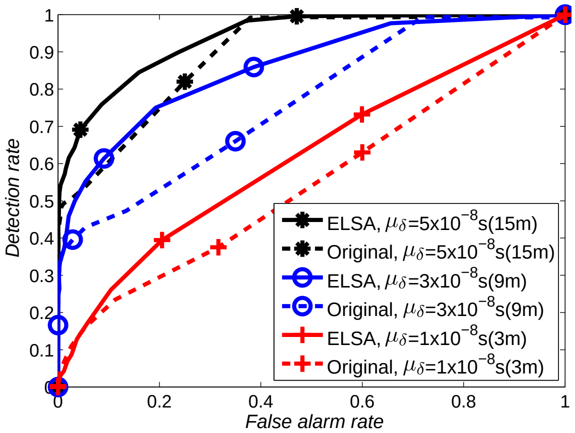


Fig. 7: ROC curves for different attack mean μ_δ with three anchors.

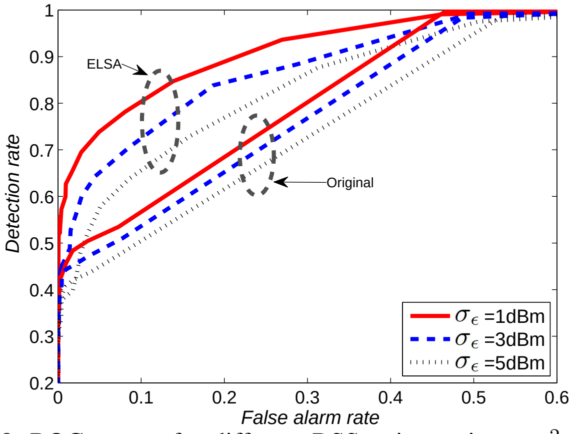


Fig. 8: ROC curves for different RSS noise variance σ_ϵ^2 with three anchors.

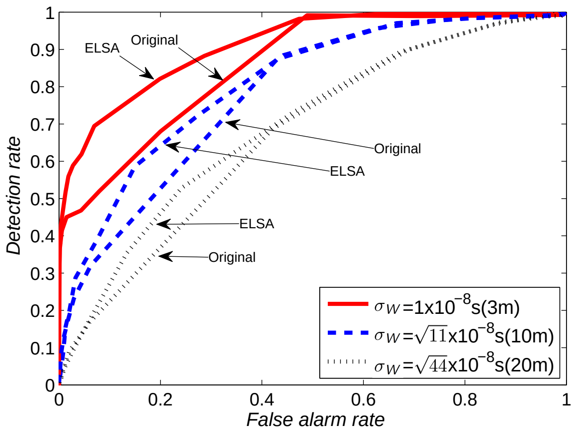


Fig. 9: ROC curves for different TOA noise variance σ_W^2 with three anchors.

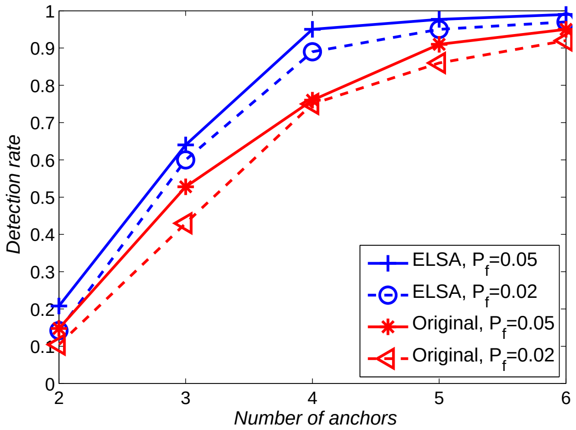


Fig. 10: Detection rates for different number of anchors with fixed false alarm rates ($\mathrm{P_f}$) of 0.02 and 0.05.

received by the anchors and the target is on the range of exactly two audible anchors. From Fig. 6, the ROC curve for ELSA indicates a significantly better detection rate which demonstrates the superiority of our approach. Despite a slight model mismatch, an attacker who only adds positive delays does not significantly degrade the detection rate of ELSA. The detection performance of the conventional approach however, is lower than ELSA's as it is difficult to detect the attack without making use of additional observations from a third anchor. Despite not receiving any observations from the third anchor, this piece of valuable information itself is exploited by ELSA whereas the conventional approach simply ignores this. As it is unlikely that the attacker is able to reduce the propagation delay of a radio wave signal, we only used a positive attacker delay (considered by most works in the literature [6], [9], [15], [21], [22]) in our comparisons.

2) ROC Curve Performance under Different Conditions: Next, we evaluate the performance of the GLRT tests for different $\mu_\delta, \sigma_\epsilon, \sigma_W$ parameters and randomize the target locations for each iteration. The chosen signal receiving threshold λ includes different inaudible scenarios depending on the target location. In Fig. 7, we plot the ROC curves for different attacker delay mean μ_δ values. A higher μ_δ value will perturb the delay measurements further and increase the spoofed distance of the target at the expense of increased detection rate by the GLRT test. Similar to Fig. 6, the detection performance of the conventional GLRT test is worse than ELSA's. As $\mu_\delta > 5 \times 10^{-8}s$ (15m approx. - take the delay and multiply it with v_p), the detection rate for ELSA is go nearer to 100% and thus we do not plot further.

In Fig. 8, we vary the RSS noise variance σ_ϵ^2 and verify that the proposed ELSA can still function correctly under large noise variances. Note that the performance of the conventional non-audibility aware GLRT test is largely unaffected by the RSS noise variance. However, the performance of ELSA depends more heavily on the RSS readings due to its reliance on audibility information. In Fig. 9, we vary the TOA noise variance σ_W^2. The detection rates for both tests drops as σ_W^2 increases because the attacker's delay is covered by in the TOA observation noise. Hence, the impact of the attack also drops when the σ_W^2 is high. Next, we increase the number of deployed anchors and plot the detection performance in Fig. 10 for fixed false alarm rates. We place an anchor at each corner of the $100\mathrm{m} \times 100\mathrm{m}$ area and another two anchors in the middle. Similarly, the detection rate of the conventional approach is less than the proposed ELSA's as it does not account for audibility. However, the detection rates for both tests will improve with diminishing returns as the number of anchors increases.

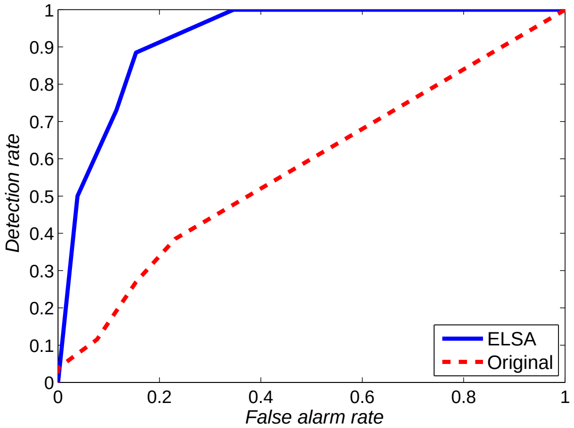


Fig. 11: ROC curves with $\lambda = -61\mathrm{dBm}$ and 41 different target locations (real-life dataset) and three anchors.

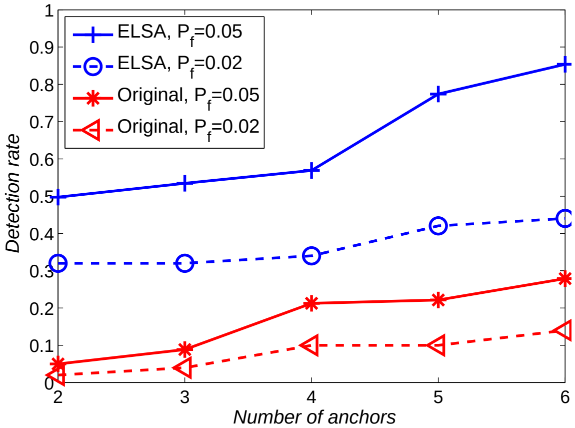


Fig. 12: Detection rates for different number of anchors (real-life dataset) with $\lambda = -61\mathrm{dBm}$ for false alarm rates ($\mathrm{P_f}$) of 0.02 and 0.05.

B. Results from Real-Life Dataset

We adopt a real sensor network TOA and RSS measurements dataset used in Patwari *et al.*'s works [38], [44] to validate our proposed audibility framework. The considered network consisted of 44 sensor nodes distributed in an office area in Motorola Labs' Florida Communications Research Lab, in Plantation, FL. Both TOA and RSS measurements were recorded between each sensor node and a high SNR was maintained throughout the experiment to ensure the reliability of the recorded data. Additional implementation details can be found in the paper [38]. The used dataset is available from the author's website [42]. We set the minimum signal receiving threshold λ to add inaudible scenarios and evaluated the performances of ELSA and the conventional approach under different scenarios. We use three of the anchors (node numbers 10, 35, 44) as used by the original authors and an attacker mean of $\mu_\delta = 1.5\times10^{-8}$ (4.5m approx.). The anchors are located at the corners of the testbed.

1) ROC Curve Performance: In Fig. 11, we plot the ROC curves for $\lambda = -61$ dBm. The chosen scenario includes a good mix of different numbers of audible anchors and highlights the superiority of our detection test compared to the conventional GLRT test which does not account for audibility. For a fixed false alarm rate, ELSA has a significantly higher detection rate. The ROC curve for the conventional GLRT test however, is closer to the diagonal line at low false alarm rates which indicates its poorer detection rate trade-off. A higher μ_δ parameter will lead to a steeper ROC curve for both schemes with the proposed scheme still being superior. In Fig. 12, we vary the number of deployed anchors and plot the detection rates of the tests for a fixed false alarm rate. Note that the detection rates for ELSA is significantly better than the rates taken from our simulation. This could be due to the limited target locations and their clustered distribution in the dataset whereas in our simulation, we uniformly picked the location of each target in each iteration.

VI. Conclusion

A new audibility-based framework has been introduced in this paper for detecting location spoofing attempts. We showed how the conventional TOA-based method may not be able to detect location spoofing attempts during inaudible scenarios and developed an audibility-aware detection test called ELSA to do so. ELSA is able to overcome outage scenarios by exploiting their implicit audibility information. In addition, we have also demonstrated that ELSA has a better detection rate compared to the conventional GLRT test using experimental results from both simulations and a real-life data set. ELSA also accommodates usage of low-cost IoT devices and lessens the need to deploy a dense network of anchors. A future research direction would be to investigate other deployment environment-specific TOA and RSS-based models to further improve existing detection rates.

Appendix

A. GLRT Test Statistic without Audibility Considerations

Consider the case where only l out of the n deployed anchors receive a delay measurement from the target node. Under the null hypothesis $\mathcal{H}_0$, the likelihood function is simply

$$p(\mathbf{t}|\mathcal{H}_0, \widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}}) = \prod_{i=1}^{l} \mathcal{N}(t_i; \frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}}, \mathbf{x}_i)}{v_p}, \sigma_W^2). \tag{15}$$

Under the alternative hypothesis $\mathcal{H}_1$, the likelihood function is given by

$$p(\mathbf{t}|\mathcal{H}_1, \widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}}) = \prod_{i=1}^{n} \mathcal{N}(t_i; \frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}}, \mathbf{x}_i)}{v_p} + \mu_\delta, \sigma_W^2 + \sigma_\delta^2). \tag{16}$$

We obtain the test statistic

$$\begin{aligned}\Lambda(\mathbf{t}) &= \frac{p(\mathbf{t}|\mathcal{H}_1, \widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}})}{p(\mathbf{t}|\mathcal{H}_0, \widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}})} \\ &= \frac{\prod_{i=1}^{l} \frac{1}{\sqrt{2\pi(\sigma_W+\sigma_\delta)}} \exp\{-\frac{1}{2(\sigma_W^2+\sigma_\delta^2)}(t_i - \frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_1}_{\mathrm{MAP}}, \mathbf{x}_i)}{v_p})^2\}}{\prod_{i=1}^{l} \frac{1}{\sqrt{2\pi}\sigma_W} \exp\{-\frac{1}{2\sigma_W^2}(t_i - \frac{d(\widehat{\mathbf{\Theta}}^{\mathcal{H}_0}_{\mathrm{MAP}}, \mathbf{x}_i)}{v_p})^2\}} \\ &\overset{\mathcal{H}_1}{\underset{\mathcal{H}_0}{\gtrless}} \eta. \end{aligned} \tag{17}$$

$$\begin{aligned}\xi = 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\Bigg[&\sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda - P_t + 10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)\right) + \sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right) \\ &- \sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right) - \sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\Bigg].\end{aligned} \tag{14}$$

B. Proof of Theorem 1

Proof. We let the distance related terms, $\psi_i = \frac{d(\mathbf{\Theta},\mathbf{x}_i)}{v_p}$, $\psi_i' = \frac{d(\mathbf{\Theta},\mathbf{x}_i)}{d_0}$, and $\mu' = \frac{\mu_\delta}{d_0}$. It can be shown that the detection and false alarm rates for the conventional GLRT test without audibility considerations are given by

$$P_{d|\psi}^{\mathrm{NA}} = \int_{\gamma}^{\infty} f(z|\mathcal{H}_1,\psi)dz,$$

$$P_{f|\psi}^{\mathrm{NA}} = \int_{\gamma}^{\infty} f(z|\mathcal{H}_0,\psi)dz.$$

respectively (see Appendix C) where γ is a threshold, l is the number of received delay measurements. On the other hand, the detection and false alarm rates for the proposed audibility-aware GLRT test are given by

$$P_{d|\psi}^{\mathrm{A}} = \int_{\gamma}^{\infty} f(z+\xi|\mathcal{H}_1,\psi)dz,$$

$$P_{f|\psi}^{\mathrm{A}} = \int_{\gamma}^{\infty} f(z|\mathcal{H}_0,\psi)dz,$$

respectively (see Appendix D) where the term ξ (from Eq. (29)) consists of the audibility-related probabilities. Note that the false alarm rates for both cases are the same,

$$P_{f|\psi}^{\mathrm{A}} = P_{f|\psi}^{\mathrm{NA}} = \int_{\gamma}^{\infty} f(z|\mathcal{H}_0,\psi)dz.$$

Hence, it can be seen that for a fixed false alarm rate $P_{f|\psi}$, the detection rates

$$P_{d|\psi}^{\mathrm{A}} \geq P_{d|\psi}^{\mathrm{NA}},$$

if $\xi \leq 0$ holds since the complementary cdf function in $P_{d|\psi}^{\mathrm{A}}$ and $P_{d|\psi}^{\mathrm{NA}}$ has a decreasing mapping.

Suppose that $\xi \leq 0$ and $\mu_\delta > 0$ (which is true in our model). From Eq. (29), the ξ term can be expressed as Eq. (14).

Next, we simplify the equation to obtain:

$$\begin{aligned}\xi = &\sum_{i=1}^{l}\ln\frac{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)}{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} \\ &+\sum_{i=l+1}^{n}\ln\frac{\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right)}{\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} \leq 0.\end{aligned} \tag{18}$$

Since $\mu_\delta > 0$, then $\mu' = \frac{\mu_\delta}{d_0} > 0$ as $d_0 > 0$. Because the logarithm function is strictly increasing for positive inputs, we have

$$\Phi\left(\log(\psi_i'-\mu')\right) < \Phi\left(\log(\psi_i')\right) < \Phi\left(\log(\psi_i'+\mu')\right).$$

Similarly, this implies that the terms

$$\frac{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)}{1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} < 1,$$

and

$$\frac{\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right)}{\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)} < 1.$$

Since the natural logarithmic function always has a negative value when the inputs are less than 1 and ξ consists of the summation of negative terms, hence, the statement $\xi \leq 0$ must be true and $P_{d|\psi}^{\mathrm{A}} \geq P_{d|\psi}^{\mathrm{NA}}$.

Subsequently, we can marginalize $P_{d|\psi_i}$ over all possible ψ_i values to obtain

$$P_d = \int P_{d|\psi_i} \times p(\psi_i)\, d\psi_i.$$

Therefore, for a fixed P_f, the following inequalities hold:

$$P_d^{\mathrm{A}} \geq P_d^{\mathrm{NA}},$$

since their equivalent representations,

$$\begin{aligned}&\int_{\psi}\int_{\gamma}^{\infty} f(z+\xi|\mathcal{H}_1,\psi)p(\psi_i)\ dz d\psi_i \\ &\geq \int_{\psi}\int_{\gamma}^{\infty} f(z|\mathcal{H}_1,\psi)p(\psi_i)dz d\psi_i,\end{aligned}$$

where the following has already been proven to be true:

$$\int_{\gamma}^{\infty} f(z+\xi|\mathcal{H}_1,\psi)dz \geq \int_{\gamma}^{\infty} f(z|\mathcal{H}_1,\psi)dz.$$

Hence, we complete the proof. □

C. Derivation of Detection and False Alarm Probabilities without Audibility Considerations

We denote the distance-related term as

$$\psi_i = \frac{d(\mathbf{\Theta},\mathbf{x}_i)}{v_p}. \tag{19}$$

We obtain the test statistic which does not take into account audibility as follows:

$$\begin{aligned}&\Lambda(\mathbf{t}) \\ &= \frac{\prod_{i=1}^{l}\frac{1}{\sqrt{2\pi}(\sigma_W+\sigma_\delta)}\exp\{-\frac{1}{2(\sigma_W^2+\sigma_\delta^2)}(t_i-\psi_i-\mu_\delta)^2\}}{\prod_{i=1}^{l}\frac{1}{\sqrt{2\pi}\sigma_W}\exp\{-\frac{1}{2\sigma_W^2}(t_i-\psi_i)^2\}} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta.\end{aligned} \tag{20}$$

Taking the logarithm on both sides, we obtain Eq. (21).

$$
\begin{aligned}
&\sum_{i=1}^{l} \ln \frac{1}{\sqrt{2\pi}(\sigma_W+\sigma_\delta)} - \sum_{i=1}^{l} \frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)} - \sum_{i=1}^{l} \ln \frac{1}{\sqrt{2\pi}\sigma_W} + \sum_{i=1}^{l} \frac{(t_i-\psi_i)^2}{2\sigma_W^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln\eta \\
&\ln \frac{\sigma_W}{(\sigma_W+\sigma_\delta)} - \sum_{i=1}^{l} \frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)} + \sum_{i=1}^{l} \frac{(t_i-\psi_i)^2}{2\sigma_W^2} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln\eta \\
&\ln \frac{\sigma_W}{(\sigma_W+\sigma_\delta)} + \sum_{i=1}^{l} \frac{(\sigma_W^2+\sigma_\delta^2)(t_i^2+\psi_i^2-2t_i\psi_i) - \sigma_W^2(t_i^2+\mu_\delta^2+\psi_i^2-2\psi_i t_i-2t_i\mu_\delta+2\psi_i\mu_\delta)}{2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln\eta \\
&\ln \frac{\sigma_W}{(\sigma_W+\sigma_\delta)} + \sum_{i=1}^{l} \frac{\sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i + \sigma_\delta^2\psi_i^2 - 2\psi_i\mu_\delta\sigma_W^2 - \mu_\delta^2\sigma_W^2}{2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)} \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \ln\eta \\
&\sum_{i=1}^{l} \sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} 2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\ln\left(\frac{\eta(\sigma_W+\sigma_\delta)}{\sigma_W}\right) + \sum_{i=1}^{l} 2\psi_i\mu_\delta\sigma_W^2 + \mu_\delta^2\sigma_W^2 - \sigma_\delta^2\psi_i^2 \\
&\sum_{i=1}^{l} \sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i \underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \gamma.
\end{aligned}
\tag{21}
$$

Now, let $\mathcal{Z} = \sum_{i=1}^{l} \sigma_\delta^2 t_i^2 + 2\mu_\delta\sigma_W^2 t_i - 2\sigma_\delta^2\psi_i t_i$ and γ be the threshold. The detection probability for the non-audibility-aware GLRT test is given by

$$
\begin{aligned}
P_{d|\psi}^{\mathrm{NA}} &= p(z > \gamma | \mathcal{H}_1, \psi) \\
&= \int_{\gamma}^{\infty} f(z|\mathcal{H}_1, \psi) dz,
\end{aligned}
\tag{22}
$$

and the false alarm probability is given by

$$
\begin{aligned}
P_{f|\psi}^{\mathrm{A}} &= p(z > \gamma | \mathcal{H}_0, \psi) \\
&= \int_{\gamma}^{\infty} f(z|\mathcal{H}_0, \psi) dz.
\end{aligned}
\tag{23}
$$

D. Derivation of Detection and False Alarm Probabilities with Audibility Considerations

From the test statistic derived in Eq. (13), we obtain:

$$
\begin{aligned}
&\Lambda(\mathbf{t}, \mathbf{r}) \\
&= \prod_{i=1}^{n} \mathcal{N}(t_i; \psi_i + \mu_\delta, \sigma_W^2 + \sigma_\delta^2)\mathbb{1}(r_i = 1) + \mathbb{1}(r_i = 0) \\
&\times \prod_{i=1}^{n} \Big[P(r_i = 1|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_1})\mathbb{1}(r_i = 1) \\
&+ P(r_i = 0|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_1})\mathbb{1}(r_i = 0) \Big] \\
&\div \prod_{i=1}^{n} \mathcal{N}(t_i; \psi_i, \sigma_W^2)\mathbb{1}(r_i = 1) + \mathbb{1}(r_i = 0) \\
&\div \prod_{i=1}^{n} \Big[P(r_i = 1|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_0})\mathbb{1}(r_i = 1) \\
&+ P(r_i = 0|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_0})\mathbb{1}(r_i = 0) \Big] \\
&\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}} \eta.
\end{aligned}
\tag{24}
$$

We further let $\psi_i' = \frac{d(\mathbf{\Theta}, \mathbf{x}_i)}{d_0}$ and $\mu' = \frac{\mu_\delta}{d_0}$ to obtain the following audibility related equations under $\mathcal{H}_0$:

$$
\begin{aligned}
P(r_i = 0|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_0}) &= \Phi\left(\frac{\lambda - P_t + 10\alpha\log\psi_i'}{\sigma_\epsilon}\right), \\
P(r_i = 1|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_0}) &= 1 - \Phi\left(\frac{\lambda - P_t + 10\alpha\log\psi_i'}{\sigma_\epsilon}\right).
\end{aligned}
\tag{25}
$$

Under $\mathcal{H}_1$, the adversary adds additional delays to the delay measurements such that the estimated distance to an anchor will be enlarged if the anchor receives a measurement and decreased if there is an inaudible scenario. The latter is due to the fact that if the estimated target location will tend to be closer towards the inaudible anchors as illustrated in Fig. 1. As such, we obtain:

$$
\begin{aligned}
P(r_i = 0|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_1}) &= \Phi\left(\frac{\lambda - P_t + 10\alpha\log(\psi_i' - \mu')}{\sigma_\epsilon}\right), \\
P(r_i = 1|\widehat{\mathbf{\Theta}}_{\mathrm{MAP}}^{\mathcal{H}_1}) &= 1 - \Phi\left(\frac{\lambda - P_t + 10\alpha\log(\psi_i' + \mu')}{\sigma_\epsilon}\right).
\end{aligned}
\tag{26}
$$

Substituting the above audibility terms into Eq. (24) and taking logarithm on both sides, the test statistic becomes

$$\begin{aligned}
&\sum_{i=1}^{l}\ln\frac{1}{\sqrt{2\pi}(\sigma_W+\sigma_\delta)}-\sum_{i=1}^{l}\frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)}\\
&+\sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)\right)\\
&+\sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right)\\
&-\left[\sum_{i=1}^{l}\ln\frac{1}{\sqrt{2\pi}\sigma_W}-\sum_{i=1}^{l}\frac{(t_i-\psi_i)^2}{2\sigma_W^2}\right.\\
&+\sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right)\\
&\left.+\sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right]\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\ln\eta.
\end{aligned}\tag{27}$$

Next, we simplify and rearrange the terms to get

$$\begin{aligned}
&\ln\frac{\sigma_W}{(\sigma_W+\sigma_\delta)}-\sum_{i=1}^{l}\frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)}+\sum_{i=1}^{l}\frac{(t_i-\psi_i)^2}{2\sigma_W^2}\\
&+\left[\sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'+\mu')}{\sigma_\epsilon}\right)\right)\right.\\
&+\sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log(\psi_i'-\mu')}{\sigma_\epsilon}\right)\\
&-\sum_{i=1}^{l}\ln\left(1-\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right)\\
&\left.-\sum_{i=l+1}^{n}\ln\Phi\left(\frac{\lambda-P_t+10\alpha\log\psi_i'}{\sigma_\epsilon}\right)\right]\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\ln\eta.
\end{aligned}\tag{28}$$

Finally, we obtain

$$\begin{aligned}
&\ln\frac{\sigma_W}{(\sigma_W+\sigma_\delta)}-\sum_{i=1}^{l}\frac{(t_i-\psi_i-\mu_\delta)^2}{2(\sigma_W^2+\sigma_\delta^2)}+\sum_{i=1}^{l}\frac{(t_i-\psi_i)^2}{2\sigma_W^2}+\sum_{i=1}^{n}\xi_i\\
&\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}2\sigma_W^2\ln\eta,\\
&\sum_{i=1}^{l}\sigma_\delta^2t_i^2+2\mu_\delta\sigma_W^2t_i-2\sigma_\delta^2\psi_it_i+2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\sum_{i=1}^{n}\xi_i\\
&\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\ln\left(\frac{\eta(\sigma_W+\sigma_\delta)}{\sigma_W}\right)\\
&\quad+\sum_{i=1}^{l}2\psi_i\mu_\delta\sigma_W^2+\mu_\delta^2\sigma_W^2-\sigma_\delta^2\psi_i^2,\\
&\sum_{i=1}^{l}\sigma_\delta^2t_i^2+2\mu_\delta\sigma_W^2t_i-2\sigma_\delta^2\psi_it_i+2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\sum_{i=1}^{n}\xi_i\underset{\mathcal{H}_0}{\overset{\mathcal{H}_1}{\gtrless}}\gamma.
\end{aligned}\tag{29}$$

where ξ_i is some function of the audibility terms (fourth term of Eq. (28) in [.] brackets) and is independent of the delay measurements $\mathbf{t}$. Using the same $\mathcal{Z}=\sum_{i=1}^{l}\sigma_\delta^2t_i^2+2\mu_\delta\sigma_W^2t_i-2\sigma_\delta^2\psi_it_i$ and γ as the previous appendix C, and let $\xi=2\sigma_W^2(\sigma_W^2+\sigma_\delta^2)\sum_{i=1}^{n}\xi_i$, the detection probability for the audibility-aware GLRT test is given by

$$\begin{aligned}
P_{d|\psi}^{\mathrm{A}}&=p(z+\xi>\gamma|\mathcal{H}_1,\psi)\\
&=\int_{\gamma}^{\infty}f(z+\xi|\mathcal{H}_1,\psi)dz,
\end{aligned}\tag{30}$$

and the false alarm probability is given by

$$\begin{aligned}
P_{f|\psi}^{\mathrm{A}}&=p(z>\gamma|\mathcal{H}_0,\psi)\\
&=\int_{\gamma}^{\infty}f(z|\mathcal{H}_0,\psi)dz,
\end{aligned}\tag{31}$$

as $\xi|\mathcal{H}_0=0$ due to the audibility terms being canceled out by each other when $\mu_\delta=0$.

References

[1] R. Hasan, R. Khan, S. Zawoad, and M. Haque, "WORAL: A witness oriented secure location provenance framework for mobile devices," *IEEE Transactions on Emerging Topics in Computing*, vol. PP, no. 1, pp. 1–13, 2015.

[2] S. Yan, R. Malaney, I. Nevat, and G. Peters, "An information theoretic location verification system for wireless networks," in *IEEE GLOBECOM*, Dec 2012, pp. 5415–5420.

[3] ——, "Optimal information-theoretic wireless location verification," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 7, pp. 3410–3422, Sept 2014.

[4] ——, "Timing information in wireless communications and optimal location verification frameworks," in *Communications Theory Workshop (AusCTW), 2014 Australian*, Feb 2014, pp. 144–149.

[5] ——, "Location verification systems for VANETs in Rician fading channels (accepted)," *IEEE Transactions on Vehicular Technology*.

[6] O. Abumansoor and A. Boukerche, "A secure cooperative approach for nonline-of-sight location verification in vanet," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 1, pp. 275–285, Jan 2012.

[7] F. Malandrino, C. Borgiattino, C. Casetti, C.-F. Chiasserini, M. Fiore, and R. Sadao, "Verification and inference of positions in vehicular networks through anonymous beaconing," *IEEE Transactions on Mobile Computing*, vol. 13, no. 10, pp. 2415–2428, Oct 2014.

[8] M. Fiore, C. Ettore Casetti, C. Chiasserini, and P. Papadimitratos, "Discovery and verification of neighbor positions in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 12, no. 2, pp. 289–303, Feb 2013.

[9] T. Leinmuller, E. Schoch, and F. Kargl, "Position verification approaches for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 13, no. 5, pp. 16–21, Oct 2006.

[10] N. Patwari, J. N. Ash, S. Kyperountas, A. O. H. III, R. L. Moses, and N. S. Correal, "Locating the nodes: cooperative localization in wireless sensor networks," *IEEE Signal Processing Magazine*, vol. 22, no. 4, pp. 54–69, July 2005.

[11] S. Capkun, K. Bonne Rasmussen, M. Cagalj, and M. Srivastava, "Secure location verification with hidden and mobile base stations," *IEEE Transactions on Mobile Computing*, vol. 7, no. 4, pp. 470–483, Apr 2008.

[12] E. Xu, Z. Ding, and S. Dasgupta, "Source localization in wireless sensor networks from signal time-of-arrival measurements," *IEEE Transactions on Signal Processing*, vol. 59, no. 6, pp. 2887–2897, June 2011.

[13] Y. Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 5, pp. 938–950, May 2013.

[14] A. Boukerche, H. Oliveira, E. Nakamura, and A. Loureiro, "Secure localization algorithms for wireless sensor networks," *Communications Magazine, IEEE*, vol. 46, no. 4, pp. 96–101, Apr 2008.

[15] S. Misra, G. Xue, and S. Bhardwaj, "Secure and robust localization in a wireless ad hoc environment," *IEEE Transactions on Vehicular Technology*, vol. 58, no. 3, pp. 1480–1489, Mar 2009.

[16] P. Yang, “PRLS-INVES: A general experimental investigation strategy for high accuracy and precision in passive RFID location systems,” *IEEE Internet of Things Journal*, vol. 2, no. 2, pp. 159–167, Apr 2015.

[17] D. Zhang, S. Zhao, L. Yang, M. Chen, Y. Wang, and H. Liu, “Nextme: Localization using cellular traces in internet of things,” *IEEE Transactions on Industrial Informatics*, vol. 11, no. 2, pp. 302–312, Apr 2015.

[18] H. Liu, H. Darabi, P. Banerjee, and J. Liu, “Survey of wireless indoor positioning techniques and systems,” *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, vol. 37, no. 6, pp. 1067–1080, Nov 2007.

[19] I. Guvenc and C.-C. Chong, “A survey on TOA based wireless localization and NLOS mitigation techniques,” *IEEE Communications Surveys Tutorials*, vol. 11, no. 3, pp. 107–124, Aug 2009.

[20] “IEEE Standard for IEEE Amendment to Part 15.3: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for High Rate Wireless Personal Area Networks (WPAN): Amendment to MAC Sublayer,” *IEEE Std 802.15.3b-2005 (Amendment to IEEE Std 802.15.3-2003)*, 2006.

[21] J. Chiang, J. Haas, J. Choi, and Y.-C. Hu, “Secure location verification using simultaneous multilateration,” *IEEE Transactions on Wireless Communications*, vol. 11, no. 2, pp. 584–591, Feb 2012.

[22] N. Basilico, N. Gatti, M. Monga, and S. Sicari, “Security games for node localization through verifiable multilateration,” *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 1, pp. 72–85, Jan 2014.

[23] J. Neyman and E. S. Pearson, “On the problem of the most efficient tests of statistical hypotheses,” *Philosophical Transactions of the Royal Society of London. Series A, Containing Papers of a Mathematical or Physical Character*, vol. 231, pp. 289–337, 1933.

[24] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Win, “Ranging with ultrawide bandwidth signals in multipath environments,” *Proceedings of the IEEE*, vol. 97, no. 2, pp. 404–426, Feb 2009.

[25] H. Wymeersch, S. Maranò, W. M. Gifford, and M. Z. Win, “A machine learning approach to ranging error mitigation for uwb localization,” *Communications, IEEE Transactions on*, vol. 60, no. 6, pp. 1719–1728, 2012.

[26] T. He, C. Huang, B. M. Blum, J. A. Stankovic, and T. Abdelzaher, “Range-free localization schemes for large scale sensor networks,” in *ACM MobiCom*, Sept 2003, pp. 81–95.

[27] P. Technology, *Pixie Location of Things Platform Introduction*, 2015 (accessed August 28, 2015). [Online]. Available: https://www.getpixie.com/

[28] DecaWave, *ScenSor DW1000 - DecaWave’s Precise Indoor Location and Communication Chip*, 2015 (accessed August 28, 2015). [Online]. Available: http://www.decawave.com/products/overview

[29] S. Capkun, M. Cagalj, G. Karame, and N. Tippenhauer, “Integrity regions: Authentication through presence in wireless networks,” *IEEE Transactions on Mobile Computing*, vol. 9, no. 11, pp. 1608–1621, Nov 2010.

[30] L. Taponecco, P. Perazzo, A. D’Amico, and G. Dini, “On the feasibility of overshadow enlargement attack on ieee 802.15.4a distance bounding,” *IEEE Communications Letters*, vol. 18, no. 2, pp. 257–260, February 2014.

[31] O. H. Abdelrahman and E. Gelenbe, “Signalling storms in 3g mobile networks,” in *IEEE International Conference on Communications (ICC)*, 2014, pp. 1017–1022.

[32] M. Pavloski and E. Gelenbe, “Mitigating for signalling attacks in UMTS networks,” in *Information Sciences and Systems - Proceedings of the 29th International Symposium on Computer and Information Sciences (ISCIS)*, 2014, pp. 159–165.

[33] P. P. C. Lee, T. Bu, and T. Woo, “On the detection of signaling dos attacks on 3g/wimax wireless networks,” *Comput. Netw.*, vol. 53, no. 15, pp. 2601–2616, Oct. 2009.

[34] D. B. Rubin, “Inference and missing data,” *Biometrika*, vol. 63, no. 3, pp. 581–592, 1976.

[35] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2001.

[36] “IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs): Amendment 1: Add Alternate PHYs,” *IEEE Std. 802.15.4a-2007*, 2007.

[37] S. Lanzisera, D. Zats, and K. Pister, “Radio frequency time-of-flight distance measurement for low-cost wireless sensor localization,” *IEEE Sensors Journal*, vol. 11, no. 3, pp. 837–845, Mar 2011.

[38] N. Patwari, A. Hero, M. Perkins, N. Correal, and R. O’Dea, “Relative location estimation in wireless sensor networks,” *IEEE Transactions on Signal Processing*, vol. 51, no. 8, pp. 2137–2148, Aug 2003.

[39] “IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low Rate Wireless Personal Area Networks (WPANs),” *IEEE Std 802.15.4-2006 (Revision of IEEE Std 802.15.4-2003)*, 2006.

[40] Z. Lu, W. Wang, and C. Wang, “From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic,” in *IEEE INFOCOM*, Apr 2011, pp. 1871–1879.

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

[42] N. Patwari, A. Hero, M. Perkins, N. Correal, and R. O’Dea, *Wireless Sensor Network Localization Measurement Repository*, 2006 (accessed March 30, 2015). [Online]. Available: http://web.eecs.umich.edu/ hero/localize/

[43] *MATLAB code*, 2015 (accessed August 28, 2015). [Online]. Available: http://idonevat.wix.com/idonevat#!about2/c1hlk

[44] N. Patwari and S. K. Kasera, “Robust location distinction using temporal link signatures,” in *ACM MobiCom*, Sept 2007, pp. 111–122.