Geo-spatial LocationSpoofing 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), which can be implemented at the backend server without modifying existing legacy IoT systems. ELSA is based on a statistical decision theory framework and uses two-way time-of-arrival (TW-TOA) information between the user’s device and the anchors. In addition to the TW-TOA information, ELSA exploits the implicit audibility information (or outage information) to improve detection rates of location spoofing attacks. Given TW-TOA and audibility information, we derive the decision rule for the verification of the device’s location, based on the generalized 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-world datasets demonstrate the superior performance of ELSA compared to conventional non-audibility-aware approaches.

Index Terms—Location spoofing detection, Internet of Things, Geo-spatial tagging, Audibility, Likelihood ratio test.

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. With the expansion of the Internet of Things (IoT), more and more users are expecting reliable and trustworthy estimates of the locations of the “things” in their systems. Without reliable information, location-based services may be severely disrupted, causing inconvenience to end users or even resulting in the loss of human lives especially in hazardous applications.

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 [1]–[3]. Specifically, we focus on the TOA-based two-way ranging (TWR) protocol [1]–[3] where a target (user device or tag) 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 its location by affecting the delay measurements received by the anchors. Therefore, many location spoofing detection schemes [4]–[12] have been proposed to deal with this threat. Typically, the detection system uses trilateration (or multilateration) [1], [13] to fuse three or more distance estimates to localize a node in two dimensions [2], [8], [9], [12], reducing ambiguity in the location estimates.

However, we show that this basic requirement of obtaining distance estimates from at least three audible anchors can be relaxed — localization can often be done reliably with fewer audible anchors. Two nodes A and B are said to be audible to each other if they are able to successfully decode the transmitted signals from each other, i.e., their received signal strengths have to be above a predefined threshold in order for them to be mutually audible. This will be formally defined in Definition 2. In contrast to prior works that simply ignore inaudible anchors (e.g., the inaudible anchors are excluded from the trilateration calculations), we exploit the implicit audibility information (or outage information) to improve the location spoofing detection rate at essentially no additional cost.

Using the concept of audibility, we develop a generalized likelihood ratio test (GLRT) [14] called Enhanced Location Spoofing Detection using Audibility (ELSA) to detect location spoofing attacks. The statistical GLRT hypothesis testing technique is a well-recognized approach that can be applied to the received TOA delay measurements to distinguish an honest target from a malicious target. ELSA can be applied to a wide range of legacy IoT systems to improve localization and the detection of spoofing attempts at essentially no additional cost because it uses implicit audibility information available in conventional TOA-based localization systems. This allows our approach to be implemented solely at the backend server.
without changing existing client IoT devices or network communications protocols (see Fig. 1).

A. Related Work

Location verification schemes have mainly relied on either the TOA or received signal strength (RSS) range-based approaches. In range-based approaches, deterministic geometrical boundaries are often used to decide whether to accept or reject localization claims. Vora et al. [15] adopt a geometric approach to detect location spoofing attacks, using sharply defined boundaries for acceptance (circular zone) and rejection (polygonal zone), with an ambiguity zone between the two boundaries. Audibility is assumed to be guaranteed within the circular acceptance zone. Such deterministic methods do not account for the variance of the naturally occurring noise. Our statistical model, on the other hand, generalizes this approach by accounting for the naturally occurring observation noise via a Gaussian noise term (see (1)): \( W_i \sim \mathcal{N}(0, \sigma_{W_i}^2) \). The geometric approach is therefore a special case of our model where \( W_i \sim \mathcal{N}(0, 0) \).

In addition, several works used cryptographic security protocols and message exchanges to prevent location spoofing attacks. The work in [16] presents a framework for using witness nodes to validate the location of targets via a cryptographic asserted location proof protocol to verify their distances to the target. Next, [8] presents a similar but distributed cooperative witnesses protocol to verify location claims through a series of message exchanges. Likewise, [10] proposes a method to check if the target lies within a claimed region and whether the claimed location exceeds a reasonable bound. Distance bounding protocols (e.g., [11]) have also been proposed to verify that a target is located within a geometric region from the anchors. This is achieved by rapidly exchanging messages based on random nonces to bound the distances between the target and the anchors.

Special features such as anonymous beacons are used in [7] to verify a target location. Capkun et al. [9] further use hidden and mobile anchors not known by the adversary to verify the location of targets via a simple challenge-response scheme. Basilico et al. [12] model 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. Our work is similar to [4]–[6], [17] which use the information theoretic likelihood ratio test (LRT) approach to verify the location of targets via RSS readings. We also adopt the LRT framework but tackle the additional challenge of having the anchors localize the target themselves.

B. Our Contributions

To the best of our knowledge, this is the first attempt to model and incorporate audibility information to improve location spoofing detection using a statistical approach based on the missing-not-at-random (MNAR) [18] concept (explained in Section II). The key contributions of this paper can be summarized as follows:

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

Notation: Uppercase letters denote random variables and the corresponding lowercase letters their realizations, and bold letters represent vectors. With a slight abuse of notation, we use lowercase \( p(x) \) to represent both the probability density function (pdf) and probability mass function (pmf), and uppercase \( P(\text{“event”}) \) to represent the probability of an event. The normal pdf is represented by \( \mathcal{N}(x; \mu, \sigma^2) = \frac{1}{\sigma \sqrt{2\pi}} e^{-\frac{(x-\mu)^2}{2\sigma^2}} \), and the standard normal cdf by \( \Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{t^2}{2}} dt \). We use \( \mathbf{1}(\cdot) \) to denote the indicator function which equals one if its argument \( \cdot \) is true and zero otherwise.

Organization: The rest of this paper is organized as follows. Section II presents a motivating example for our proposed framework. The analytic model is introduced in Section III and the problem formulation is presented in Section IV. Section V discusses our experimental results. Finally, conclusions are drawn in Section VI. An extended version of this paper, including the proofs and appendices, can be found in [19].

II. Example for Proposed Audibility Framework

We first illustrate with an example the concept of audibility before elaborating how audibility aids in detecting the location spoofing attacks.

A. How Audibility Aids in Location Spoofing Detection

Using the conventional trilateration technique [1], [13] (without utilizing audibility information), distance estimates from at least three different non-collinear anchors are needed to localize a target. Otherwise, there may exist ambiguity. For example, the target 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 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 (in)audibility 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 [18] where he developed a statistical framework to account for missing data.

B. Toy Example on the Use of Audibility Information

Shown in Fig. 3 is a room with an anchor at each corner. Suppose that a malicious target at the left side of the room
Fig. 3. Proposed method where a malicious target attempts to spoof its location by adding delays to the delay measurements between the target and the anchor, denoted by $t_{\text{target, anchor}}$.

Fig. 4. Message exchanges of the two-way ranging (TWR) distance estimation protocol [21]. The two time segments marked A and B represent the possible points of attack by an adversary (see our threat model in Section III-C).

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. We adopt the widely used log-normal propagation (path loss) model [1], [20] and define audibility as follows.

**Definition 1** (Path loss model). The received signal power (in dBm) by a node A located at $\Theta_A = [x_A, y_A]$ from a signal sent by node B which is located at $\Theta_B = [x_B, y_B]$ is given by

$$P_r = P_t - 10\alpha \log \frac{d(\Theta_A, \Theta_B)}{d_0} + \epsilon_r,$$

where $P_t$ is the received power from node B at a reference distance $d_0$ (typically 1m), $\alpha$ is the path-loss exponent, $d(\Theta_A, \Theta_B) := \sqrt{(x_A - x_B)^2 + (y_A - y_B)^2}$ is the Euclidean distance between nodes A and B, and $\epsilon_r \sim N(0, \sigma^2)$ is the received power noise (due to the shadowing effect).

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

$$P_{R_B} = P_T - 10\alpha \log \frac{d(\Theta_A, \Theta_B)}{d_0} + \epsilon_r \geq \lambda,$$

where $\lambda$ is a predefined threshold representing the receiver’s sensitivity. Otherwise, it is said to be inaudible.

B. System Model

We consider a scenario where a fusion center receives some delay measurements from its anchors and transmits the measurements to a backend server for verifying a target’s location along 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 $X_i = [x_i, y_i]$. 

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 in Fig. 3, but the concept remains the same.
where its 2D coordinates \(x_i, y_i \in \mathbb{R}\) for \(i \in \{1, \ldots, n\}\).

2) The true location of the target (prover) is denoted by \(\Theta = [x_\theta, y_\theta]\),

where its 2D coordinates \(x_\theta, y_\theta \in \mathbb{R}\). Depending on the deployment scenario, we assume that there is a prior distribution \(p(\Theta)\) for the target’s location. 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 [21] is used (see Fig. 4). The anchor transmits a request packet to the target which then replies with a response packet. Each anchor \(i\) in the communication range of the target will receive a delay measurement [1] which can be represented by:

\[
t_i = \frac{d(\Theta, x_i)}{v_p} + W_i,
\]

where \(d(\Theta_A, \Theta_B)\) is the Euclidean distance between two locations \(\Theta_A\) and \(\Theta_B\), \(v_p\) 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 \(W_i \sim \mathcal{N}(0, \sigma_w^2)\).

4) In our audibility model, each anchor \(i\) in the communication range of the target will receive a signal with a received power \(P_i\) (see Definition 1) that is equal or higher than the minimum signal receiving threshold \(\lambda\):

\[
P_i = P_t - 10\alpha \log \frac{d(\Theta, x_i)}{d_0} + \epsilon_i \geq \lambda.
\]

The target is said to be audible to the anchor (see Definition 2).

5) If an anchor \(i\) does not receive any signal from the target, we can treat the received signal as having a received power \(P_i\) that is less than the minimum signal receiving threshold \(\lambda\), i.e., \(P_i < \lambda\). The target is said to be inaudible to the anchor (see Definition 2).

6) We let \(r_i\) be an indicator variable that depends on whether the anchor \(i\) receives a delay measurement from the target (see (2)):

\[
r_i = \begin{cases} 1 & \text{if } P_i \geq \lambda, \\ 0 & \text{otherwise}. \end{cases}
\]

Empirical Support for Our Models: Our chosen TOA and RSS models in (1) and (2) respectively are supported by the experimental measurements obtained from [22].

C. Threat Model

We consider an internal and external adversary whose goal is to significantly perturb a target’s perceived location by the fusion center \(\hat{\Theta}\) from its true location \(\Theta\) by manipulating the response time of the target, thus affecting the TOA delay measurements received by the anchors as discussed in our example in Section II. Recall from Section III-B that the delay measurement received at the \(i\)th anchor in a non-adversarial environment is given by (1). A malicious target or anchor (in the case of an internal adversary) can falsify the target’s location by adding a delay \(\delta_i\) before replaying to a TWR request message such that the received delay measurement becomes

\[
t_i = \frac{d(\Theta, x_i)}{v_p} + W_i + \delta_i,
\]

where we assume \(\delta_i \sim \mathcal{N}(\mu_\delta, \sigma_\delta^2)\). The malicious target can insert the delay at point A (as shown in Fig. 4) in the TWR protocol while a malicious anchor may insert the delay at point B. The malicious targets may collude to fool the anchors by appearing to be closer or further from them. This scenario is accounted by the i.i.d. Gaussian attacker delay model. The Gaussian model is used for analytical convenience as the adversary may be able to launch distance enlargement or distance reduction attacks [23]. An external adversary (which cannot compromise nodes) may increase the delay measurement by some \(\delta_i\), which may not necessarily be positive, by attacking the PHY layer [24].

IV. ELSA: ENHANCED LOCATION SPOOFING DETECTION USING AUDIBILITY

We present the location spoofing detection test Enhanced Location Spoofing Detection using Audibility (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 [14]) can be used to detect location spoofing attempts under the two competing hypotheses:

\[
H_0 : \text{no location spoofing} \\
H_1 : \text{location spoofing attempt}.
\]

The LRT\(^3\) can be formulated as:

\[
\Lambda(t, r) \triangleq \frac{p(t, r|H_1)}{p(t, r|H_0)} \overset{?}{\geq} \eta,
\]

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

Under the Neyman-Pearson lemma, the LRT is the most powerful test at each significance level \(\alpha\) (false alarm rate)

\(^2\)Note that \(W_i\) may also be from any other known parametric distribution.

\(^3\)The LRT for the conventional non-audibility-aware approach (see Appendix-A of [19]) is \(\Lambda(t) \triangleq \frac{\tilde{p}(t|H_1)}{\tilde{p}(t|H_0)} \overset{?}{\geq} \eta\).

2327-4662 (c) 2015 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission. See http://www.ieee.org/publications_standards/publications/rights/index.html for more information.
for a threshold \( \eta \) where \( p(A(t, r)|H_0) > \eta |H_0| = \alpha \). The functions \( p(t, r|H_0) \) and \( p(t, r|H_1) \) represent the likelihood functions for the null hypothesis and alternative hypothesis respectively. Since we treat \( \Theta \) as an unknown random variable, the likelihood functions can be formulated as

\[
p(t, r|H_j) = \int p(t, r|\Theta, H_j)p(\Theta|H_j)\,d\Theta
\]

\[
= \int p(t|r, \Theta, H_j)p(r|\Theta, H_j)p(\Theta|H_j)\,d\Theta.
\]

However, a closed form expression to the above integral is intractable due to the non-linear relationship in \( p(t, r|\Theta, H_j) \). Hence, the LRT in (5) is no longer applicable. Instead, the likelihood functions can be formulated as

\[
\hat{\Lambda}(t, r) \triangleq \frac{p(t, r|H_1, \hat{\Theta}_{MAP}^H)}{p(t, r|H_0, \hat{\Theta}_{MAP}^H)} \gtrless \eta,
\]

where we approximate \( p(t, r|H_j) \) using the maximum-a-posteriori (MAP) estimate (see Appendix-B of [19]) given by

\[
\hat{\Theta}_{MAP}^H = \arg\max_{\Theta} \sum_{i=1}^{n} \log \mathcal{N}(t_i; \frac{d(\Theta, x_i)}{v_p} + \delta, \sigma_W^2)1(r_i = 1)
\]

\[
+ \sum_{i=1}^{n} \log P(r_i = 1|\Theta, H_j)1(r_i = 1)
\]

\[
+ P(r_i = 0|\Theta, H_j)1(r_i = 0) + \log p(\Theta|H_j).
\]

B. Derivation of Test Statistic

Under the null hypothesis \( H_0 \), the likelihood function is simply

\[
p(t, r|H_0, \hat{\Theta}_{MAP}^H) = p(t|r, H_0, \hat{\Theta}_{MAP}^H) p(r|H_0, \hat{\Theta}_{MAP}^H),
\]

where

\[
p(t|r, H_0, \hat{\Theta}_{MAP}^H) = \prod_{i=1}^{n} \left[ \mathcal{N}(t_i; \frac{d(\hat{\Theta}_{MAP}^H, x_i)}{v_p}, \sigma_W^2)1(r_i = 1) + 1(r_i = 0) \right],
\]

and

\[
p(r|H_0, \hat{\Theta}_{MAP}^H) = \prod_{i=1}^{n} \left[ P(r_i = 1|\hat{\Theta}_{MAP}^H)1(r_i = 1) + P(r_i = 0|\hat{\Theta}_{MAP}^H)1(r_i = 0) \right].
\]

Under the alternative hypothesis \( H_1 \),

\[
p(t, r|H_1, \hat{\Theta}_{MAP}^H) = p(t|r, H_1, \hat{\Theta}_{MAP}^H) p(r|H_1, \hat{\Theta}_{MAP}^H),
\]

where

\[
p(t|r, H_1, \hat{\Theta}_{MAP}^H) = \prod_{i=1}^{n} \left[ \mathcal{N}(t_i; \frac{d(\hat{\Theta}_{MAP}^H, x_i)}{v_p} + \mu, \sigma_W^2 + \sigma_{\delta}^2)1(r_i = 1) + 1(r_i = 0) \right],
\]

and

\[
p(r|H_1, \hat{\Theta}_{MAP}^H) = \prod_{i=1}^{n} \left[ P(r_i = 1|\hat{\Theta}_{MAP}^H)1(r_i = 1) + P(r_i = 0|\hat{\Theta}_{MAP}^H)1(r_i = 0) \right].
\]

Substitution of the values obtained from (8) and (9) into (6) will give the test statistic in (10). Algorithm 1 (see [19]) summarizes the steps in the proposed ELSA. Next, we prove using the following theorem that ELSA provides better detection rates than the conventional non-audibility-aware GLRT for the same false alarm rate tradeoff.

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

\[
P_d^A \geq P_d^N.
\]

**Proof.** See Appendix-C of [19]. \(\square\)

V. Experimental Results and Discussion

In this section, we evaluate the performance of our proposed detection test ELSA against the conventional GLRT (labeled as ‘original’ in the figures) which does not take into account audibility (similar to the work in [17]), in terms of the location spoofing detection performance. Both simulations and data from a real-world dataset (available in [25]) were used in our evaluation. The MATLAB code used to obtain the simulation results is available as supplemental material, which can be found at [19], [26]. Unless otherwise stated, the parameters in Table I were used in our simulations.

A. Simulation Results using 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 m \times 100 m area as shown in Fig. 2 and the target is selected uniformly at random inside this area (hence, \( p(\Theta) = \frac{1}{100^2} \times \frac{1}{100^2} \)). We used a grid search with a one meter granularity to search for the optimal target location using the MAP approach (see (7)).

1) ROC Curve Performance: We use the receiver operating characteristic (ROC) curve to compare the detection and false alarm performance of ELSA, against the conventional non-audibility-aware GLRT. For a given decision rule \( \eta \), the detection rate is given by

\[
P(\Lambda(t, r) > \eta|H_1),
\]

and the false alarm rate is given by

\[
P(\Lambda(t, r) > \eta|H_0).
\]

In Fig. 5, we plot the ROC curves for scenarios when an attacker adds a positive delay to the delay measurements
\[ \Lambda(t, r) = \prod_{i=1}^{n} N(t_i; \frac{d(\hat{H}_i^E, x_i)}{\nu_p} + \mu_W^2 + \sigma_W^2, \sigma_W^2 I(r_i = 1) + I(r_i = 0) ) \]

\[ \times \left[ \prod_{i=1}^{n} P(r_i = 1|\hat{H}_i^E) I(r_i = 1) + P(r_i = 0|\hat{H}_i^E) I(r_i = 0) \right] \left[ \prod_{i=1}^{n} N(t_i; \frac{d(\hat{H}_i^O, x_i)}{\nu_p} + \sigma_W^2, \sigma_W^2 I(r_i = 1) + I(r_i = 0) ) \right] \]

\[ \times \left[ \prod_{i=1}^{n} P(r_i = 1|\hat{H}_i^O) I(r_i = 1) + P(r_i = 0|\hat{H}_i^O) I(r_i = 0) \right] \]

(10)

Fig. 5. ROC curves for three anchors, of which two are audible (see Fig. 2).

Fig. 6. ROC curves for different attacker delay mean \( \mu_\delta \) with three anchors.

Fig. 7. ROC curves for different RSS noise variance \( \sigma_W^2 \) with three anchors.

Fig. 8. ROC curves for different TOA noise variance \( \sigma_V^2 \) with three anchors.

received by the anchors and the target is in the range of exactly two audible anchors. The ROC curve for ELSA indicates a significantly better detection performance compared to the conventional approach where it is difficult to detect the attack without making use of additional information from the third anchor. Despite a slight model mismatch, an attacker who only adds positive delays does not significantly degrade the detection rate of ELSA.

2) ROC Curve Performance under Different Conditions: Next, we evaluate the performance of the GLRT tests for different \( \mu_\delta, \sigma_\nu, \sigma_W \) parameters and randomize the target locations for each iteration. The chosen signal receiving threshold \( \lambda \) includes different inaudible scenarios depending on the target location. In Fig. 6, we plot the ROC curves for different attacker delay mean \( \mu_\delta \) values. A higher \( \mu_\delta \) value perturbs the delay measurements further and increases the spoofed distance of the target at the expense of increased detection rate by the GLRT. Similar to Fig. 5, the detection performance of the conventional GLRT is worse than ELSA’s.

The impact of obstacles and multipaths can affect the detection performance of the proposed test by increasing the TOA observation noise variance \([22]\). Similarly, the RSS variance will also increase due to the shadowing and multipath. In Figs. 7 and 8, we vary the RSS noise variance \( \sigma_W^2 \) and TOA noise variance \( \sigma_V^2 \) respectively to verify that the proposed ELSA can still function correctly under large noise variances. Note that the performance of the conventional non-audibility aware GLRT is largely unaffected by the RSS noise variance. However, the performance of ELSA depends more heavily on the RSS readings which affect the audibility information.

In Fig. 8, the detection rates for both tests drop as \( \sigma_V^2 \) increases because the attacker delay is dominated by the TOA observation noise. Hence, the impact of the attack also drops when \( \sigma_V^2 \) is high. Next, we increase the number of deployed anchors and plot the detection performance in Fig. 9 for fixed false alarm rates. We placed an anchor at each corner of the
Fig. 9. Detection rates for different number of anchors with fixed false alarm rates \((P_f)\) of 0.02 and 0.05, using synthetic data.

Fig. 10. ROC curves with \(\lambda = -61\) dBm and 41 different target locations and three anchors, using the real-world dataset.

Fig. 11. Detection rates for different number of anchors with \(\lambda = -61\) dBm for false alarm rates \((P_f)\) of 0.02 and 0.05, using the real-world dataset.

100 m \(\times\) 100 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 performance for both tests will improve with diminishing returns as the number of anchors increases.

B. Simulation Results using Real-World Dataset

To validate our proposed audibility-aware framework, we use a real-world dataset comprising TOA and RSS measurements taken by Patwari et al. [22], [25], [27]. 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. We set the minimum signal receiving threshold \(\lambda\) to add inaudible scenarios and evaluated the performance 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 delay mean of \(\mu_\delta = 1.5 \times 10^{-8}\) s (4.5 m approx.). The anchors are located at the corners of the testbed.

ROC Curve Performance: In Fig. 10, 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 ELSA compared to the conventional GLRT. For a fixed false alarm rate, ELSA has a significantly higher detection rate. The ROC curve for the conventional GLRT, however, is closer to the diagonal line (not drawn) at low false alarm rates which indicates its poorer detection rate trade-off. In Fig. 11, we vary the number of deployed anchors and plot the detection rates of the tests for a fixed false alarm rate. ELSA offers improved detection performance compared to the conventional approach, and this improved performance is more significant in the real-world dataset compared to our synthetic data as shown in Fig. 9. This could be due to the limited target locations and their clustered distribution in the real-world dataset whereas in our synthetic data, we uniformly picked the location of each target in each iteration.

VI. CONCLUSION

A new audibility-aware 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 especially during inaudible scenarios, and developed an audibility-aware detection test called ELSA to do so. In addition, we have also demonstrated that ELSA has better detection performance compared to the conventional GLRT using experimental results with both synthetic data and a real-world dataset. A future research direction would be to investigate other deployment environment-specific TOA, RSS-based, or even energy-harvesting models to further improve existing detection performance.

REFERENCES

[3] “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.
Jing Yang Koh received the B.Eng. degree in computer engineering from Nanyang Technological University, Singapore in 2013. He is currently a Ph.D. candidate in the National University of Singapore, Singapore and attached to the Institute for Infocomm Research (I²R), Singapore. His research mainly focuses on using statistical signal processing, machine learning, and optimization techniques for wireless network security and privacy.

Ido Nevat received the B.Sc. degree in electrical engineering from the Technion-Israel Institute of Technology, Haifa, Israel in 1998 and the Ph.D. degree in Electrical Engineering from the University of Newcastle, Sydney, Australia, in 2010. From 2010-2013 he was a post doctoral research fellow with the Wireless and Networking Technologies Laboratory at CSIRO, Australia. Currently he is a team leader at the Institute for Infocomm Research (I²R), Singapore. His main areas of interests include statistical signal processing, machine learning and Bayesian statistics.

Derek Leong is a scientist with the “Sense and Sense-abilities” programme at the Institute for Infocomm Research (I²R), Singapore. He received the B.Eng. in electrical and computer engineering from Carnegie Mellon University in 2005, and the M.S. and Ph.D. degrees in electrical engineering from the California Institute of Technology in 2008 and 2013 respectively. His research and development interests include distributed systems and sensor networks.

Wai-Choong (Lawrence) Wong is Professor in the Department of Electrical and Computer Engineering, National University of Singapore (NUS). Since joining NUS in 1983, he served in various leadership positions at the department, faculty and university levels. Prior to joining NUS in 1983, he was a Member of Technical Staff at AT&T Bell Laboratories, Crawford Hill Lab, NJ, USA, from 1980 to 1983. He received the B.Sc. and Ph.D. degrees in Electrical and Computer Engineering from Loughborough University, UK. His research interests include wireless and sensor networks and systems, ambient intelligent platforms, localization and source-matched transmission techniques with over 200 publications and 5 patents in these areas. He has received several awards including the IEEE Marconi Premium Award in 1989, IEEE Millennium Award in 2000, e-nnovator Awards (Open Category) in 2000, Best Paper Award at the IEEE International Conference on Multimedia and Expo (ICME) 2006, and Best Paper Award at the 2nd International Conference on Ambient Computing, Applications, Services and Technology (AMBIENT), 2012.


