Spoofing Evident and Spoofing Deterrent Localization using Ultra-wideband (UWB) Active-Passive Ranging

Haige Chen, *Student Member, IEEE*, and Ashutosh Dhekne, *Member, IEEE*

***Abstract*— This paper presents UnSpoof, an ultra-wideband (UWB) localization system that can detect and localize distance-spoofing tags with a few collaborative passively-receiving anchors. We propose novel formulations that enable passively-receiving anchors to deduce their time-of-flight (ToF) and time-difference-of-arrival (TDoA) just by overhearing standard two-way ranging (TWR) messages between the tag and one active anchor. Our ToF formulation can be used to precisely localize an honest tag, and to detect a distance-spoofing tag that falsely reports its timestamps. Additionally, our TDoA formulation enables spoofing deterrent localization, which can be used to track down and apprehend a malicious tag. Our experimental evaluation shows 30 cm 75^{th} percentile error for ToF-based honest tag localization, and sub-meter error for TDoA-based localization for spoofing tags. We demonstrate successful detection of distance reduction and enlargement attacks inside the anchors' convex hull, and graceful degradation outside. Additionally, we show the effects of a non-regular geometry of anchors and invite researchers and practitioners to experiment with anchor topologies of interest to them via our open source modeling software.**

***Index Terms*— Location Awareness, Location Spoofing, Ultra-wideband Radios**

I. Introduction

The growing need for ubiquitous connectivity and context awareness in Internet of Things (IoT) and mobile computing is driving the development of a wide-range of technologies including indoor localization. Using radio frequency (RF) signals for indoor localization has been researched for a long time. Compared to alternative sensing modalities such as visible light, infrared and ultrasounds, RF-based indoor localization in general is well-balanced between good sensing range, robustness against obstruction, and accuracy. However, RF-based indoor localization has its own challenges because RF signals experience reflections, scattering, and attenuation from objects and building materials when propagating through the indoor environment. The emerging ultra-wideband (UWB) technology proves to be very promising for localization due to its robustness in multipath-rich environments. UWB has a large bandwidth of more than 500MHz, giving it abilities to transmit ultra-short pulses and distinguish the direct path signal from multipaths. UWB has been demonstrated to achieve high localization accuracy of 10cm in real-world experiments. Because of its promising performance, UWB has already been integrated in products and services by companies such as Apple [1], Google [2], Samsung [3], NXP [4], etc., and has started to impact our life with daily applications in object finding, keyless entry, inventory tracking, and more.

Measurement of distances, also called ranging, is a fundamental primitive in localization. However, time-of-flight (ToF) and time-difference-of-arrival (TDoA) measurements are not trivial to obtain for several reasons. Since radio frequency signals travel at the speed of light, nanoseconds to picoseconds level timing precision is required. Although the large bandwidth of UWB allows timestamping the signal arrival at a very high resolution, other source of measurement errors such as imperfect clocks also need to be taken into consideration. In practice, timestamping of the signal arrival is measured in reference to the clock of the receiver, whose frequency may drift from its nominal frequency slightly, causing non-negligible errors in the ranging measurements. Therefore, ranging protocols and formulations should be designed to mitigate the effect of clock drifts. As an example, the IEEE standard two-way ranging (TWR) formulation is proved to eliminate clock drift related errors [5].

However, a loop-hole remains in TWR—since both transceivers must report the transmission and reception times for the formulations to work, a transceiver could manipulate some of the timings that it reports and spoof its distance. Localization, if only used as a convenience for clients, such as in indoor navigation, does not typically need to deal with this vulnerability, since clients would themselves suffer from inaccurate navigation. Spoofing of distances by the client is therefore unlikely and does not affect anyone else. Such spoofing might not immediately seem lucrative. It is then natural to wonder: *is there any need to plug this falsified timestamp reporting hole at all?* UWB technology is quite mature and has been successfully deployed in several real-world settings including large industrial spaces, commercial establishments, etc. However, in most of these application use-case, both the UWB anchors and UWB tags were under the same organization's control. Take industrial IoT use-cases for

Manuscript submitted on November 1, 2023. This material is based upon work supported by the NSF under Grant No. 2145278.

Haige Chen is with Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: hchen425@gatech.edu).

Ashutosh Dhekne is with Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: dhekne@gatech.edu).

example where the anchors are deployed in the infrastructure and tags are deployed on conveyor belts, heavy equipment etc. Under such conditions both the anchors are tags are trustworthy and distance spoofing is unlikely. Similarly, when UWB is used to guide indoor navigation, while the tags might not be in the control of the same entity as the anchors, it is the tags who benefit from honest localization, once again negating any utility of distance spoofing, unless a malicious entity tampers with a different user's tag. However, the existence of an easy way to spoof distances makes a different class of applications possible; one that includes proof of distance. This includes, for example, enabling physical access control in companies via UWB smartphones or UWB smart access-cards so that workers can walk around while doors open for them without having to take out the access card and touch an RFID reader, being able to prove delivery of a package, being able to review a restaurant on social media only when one did actually visit the restaurant, and so on. Detection of distance spoofing, and possible apprehension of such a spoofing device through accurate localization despite distance spoofing, will be crucial steps in enabling provable indoor localization (other steps include improved precision of timestamps, verifiable signatures from the infrastructure anchors, etc.).

At its core, this paper develops a mechanism for spoofing evident localization where a set of trusted but passive anchor nodes helps an active anchor determine if a client has cheated on its timestamps (to spoof location). Further, the information captured by the passive anchors also allows determining the location of the client despite such manipulated timestamps, thus deterring a client from attempting spoofing in the first place. Since the passive anchors help determine location, only a single two-way ranging between the client and one active anchor is needed. In this work, we show that these properties are upheld not just inside the convex hull described by the anchors, but also, to a certain extent, outside the convex hull.

A key reason that such a mechanism can be developed is attributed to a *novel formulation* that overhearing anchors can use to keep effects of clock drifts to a minimum. Historically, formulations that mitigate clock drift effects have seen significant success exemplified by the adoption of a new formulation in the IEEE802.15.4z standard [6] by shunning the previous averaging formulation in the IEEE802.15.4a standard [7] for localization. In a completely different context, a similar improvement in the formulation of TDoA was presented in our IPIN 2022 paper in a system called PnPLoc [8]. Of course, the TDoA derivation in PnPLoc pertained to a scalable privacy preserving system for a client UWB device to obtain its own location, which is a completely different context compared to the current work. Here the infrastructure anchors wish to obtain the location of UWB clients. This is a common use-case for localization in Industrial Internet of Things (IIOT), for example, where the organization centrally monitors the location of all its assets inside the building.

We now introduce UnSpoof (depicted in Fig. 1), a system that detects distance spoofing by a participating UWB tag, allows apprehension of a spoofing device by revealing its true location despite spoofing, while providing highly accurate location of an honest tag to infrastructure anchor nodes. The

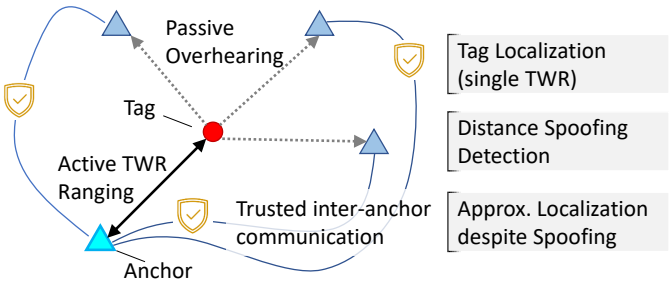


Fig. 1: UnSpoof setup includes a single active ranging tag-anchor pair. Other passively listening anchors share their observations collaboratively, which enables tag localization, detection of distance spoofing by tag, and approximate localization despite spoofing.

setting of our system is as follows: a set of UWB anchor nodes are installed such that they are all within radio range of a UWB tag present anywhere in a coverage area. The distances between the anchor nodes is known, either through calibrated UWB measurements or via physical surveying during installation. The anchors can communicate with each other securely, meaning UWB messages received from another anchor can be verified to be really from that anchor. An untrustworthy tag in the vicinity performs a *single two-way ranging message exchange* using the standard IEEE 802.15.4z protocol [9], involving the POLL, RESPONSE, and FINAL messages, *with a single infrastructure anchor*, called *active anchor*. All other anchors, called *passive anchors*, overhear the message exchange. Each overhearing anchor calculates an estimated tag-anchor distance and shares its results with the active anchor. The active anchor uses its own observations and those by the collaborating passive anchors to compute the location of the tag, by solving both time of arrival equations as well as time-difference-of-arrival equations, separately. If the tag tries to spoof the distance measurement, the inferred time-of-arrivals from the passive anchors do not match and no location can be determined. At this stage, a spoofed distance is *detected*. We then resort to a TDoA formulation that ignores the timestamps in the tag's messages and computes the tag's location, albeit with slightly less accuracy. This TDoA based location can be used to apprehend a malicious tag, thereby deterring tags from spoofing their locations in the first place. To the best of our knowledge, no other system achieves this set of attributes. Next, we will briefly dwell on the limited related work on this topic.

This work is an extension of our IPIN 2023 paper [10], allowing us to expand on several aspects including a discussion about non-regularly shaped anchor geometries. In the rest of this paper, after briefly dwelling on the related work in this space, we derive our novel formulation, show its robustness in comparison with other formulations, and then validate its effectiveness using experimental measurements using DW1000 UWB devices, simply running the standard two-way-ranging protocol. Anchors in our testbed are arranged in a regular hexagon, however, we show how our findings can be generalized by simulating realistic ranging data with

anchors placed *ad hoc* and not in a regular geometric shape. To encourage future research in this area, we have open sourced the simulation code which can be readily used for other anchor geometries based on real-world deployments.

II. Related Work

UWB is a radio technology that operates in the $3.1 - 10.6$ GHz range with bandwidth larger than 500 MHz [11]. Because of its large bandwidth, UWB is more capable of discerning direct-path signal from multipath signals compared to many other radio standards such as WiFi, Bluetooth, and Zigbee, enabling it to achieve decimeter localization accuracy and robustness in multipath-rich indoor environments [11]–[14]. The localization methods used in UWB localization can be generally categorized into ranging-based, angle-based [15]–[17], and fingerprinting-based [18], [19] approaches, where ranging-based methods can be further categorized into ToF [5], [20]–[22] and TDoA [23]–[25] approaches. In this work, we focus on the widely used TWR method that is specified in the IEEE 802.15.4 standard [9]. We observe that the emerging UWB technology is not only fueling novel IoT applications, such as virtual reality [26], robot navigation [25], tracking social interaction [27], etc. that improve the convenience and efficiency of people's lives, but also enabling more critical applications such as location-based authentication [28] and keyless access [29] with high requirement for security. Therefore, researchers have placed the security risks of localization under scrutiny [30]–[35]. Secure ranging and secure localization has been an active area of research. Researchers have found several methods to either corrupt distance measurements where an adversary directly attacks the physical layer by introducing interference [36]–[40], or spoof distance measurements where a participating tag maliciously alters timing information [41], [42]. We focus on distance spoofing where a malicious tag attempts to cheat about its location by reporting wrong timing information, which is referred to as *internal attacks* in existing literature [41], [42]. Others have previously found, similar to our results, that if overhearing trusted anchors exist, such spoofing can be *detected* [41]–[44]. However, [41], [42] focus on a single sided ranging protocol, which is quite inaccurate in face of clock drifts. In [44], the authors proposed that TDoA localization with covert base stations can prevent internal attacks, but the model considered requires synchronization between all anchors, which incurs large financial and energy cost. In [45], the authors proposed the Verifiable Multilateration method based on distance bounding, which typically requires special hardware [46]. We show that spoofing detection is possible when the system simply uses the latest IEEE 802.15.4z [9] protocol and commercial off-the-shelf (COTS) hardware. Furthermore, in contrast to most existing studies, we show that it is also possible to determine the true location of the tag despite spoofing using a time-difference of arrival formulation. Our formulation is a variation of our previous work [8], and is resistant to clock drifts and outperforms traditional formulations irrespective of turn-around time delays at the tag (or at the anchor). Existing literature only provides spoofing detection *inside the convex hull* defined by the anchors. However, we find that it is possible to detect spoofing outside the convex hull when using our ToF based validation although less robust than inside the convex hull. To the best of our knowledge, no other system has shown these properties. It is worth noting that different from [22], [47], which also achieve passive ranging by overhearing anchors, our method can extract ToF and TDoA at the same time balancing accuracy for honest tags and ability to apprehend dishonest ones.

Sym	Description
ρ	Propagation Delay
$\hat{\rho}$	Measured Propagation Delay
R	Round Trip time from sending a packet to receiving a reply
D	Reception of a packet to transmission of a response (Turn-around delay) for a node
δ	Clock-drift rate
A	Active ranging anchor
T	Active ranging tag or client device
B	Passive ranging anchor
$\Delta\hat{R}_x$	The difference in observed or spoofed time delay and the real delay as observed by x

TABLE I: Quick-guide for various symbols and notations used in this paper and their short descriptions.

III. UnSpoof System Design

The symbols we use to denote various entities in UnSpoof are summarized in Table I, which would come handy for the formulations and derivations we describe next. Please note that standard localization literature in the UWB domain is followed for the symbols and notations. As described in Section I, UnSpoof involves one active ranging tag (T), one active ranging anchor (A), and several passive listening anchors ($B^{(i)}s$). Propagation delays between the anchors (i.e. $\rho_{AB^{(1)}}, \rho_{AB^{(2)}}, ...$) are accurately known beforehand, derived from the inter-anchor distance. The tag T initiates a single two-way-ranging message exchange with the anchor A. We use ρ_{AT} to denote the wireless propagation delay between the active anchor A and tag T, which is calculated by the anchor A based on the standard IEEE 802.15.4z two-way ranging protocol (called TWR), first derived in [5]:

$$\rho_{AT} = \frac{R_T R_A - D_T D_A}{2(R_A + D_A)} \tag{1}$$

where R_x denotes the round trip delay observed by device x and D_x denotes its turn-around time to switch from a receiver to a transmitter. Note that this formulation significantly mitigates the effect of clock drift without relying on any specific timing relationship between D_T and D_A unlike the IEEE 802.15.4a standard. For a detailed analysis of this and other similar formulations, and for understanding how reliance on specific timing relationships is detrimental to the overall ranging process, the reader is referred to [48]. In TWR, a malicious tag can spoof the measurement ρ_{AT} simply by reporting untruthful timing information R_T and D_T. It is easy to show that cheating by presenting a smaller R_T and a larger D_T lead to range reduction, and a larger R_T and a smaller D_T lead to range enlargement (nanoseconds-level cheating on timings). Usually, this attack is difficult to detect as the tag can spoof its range to each anchor independently. In UnSpoof,

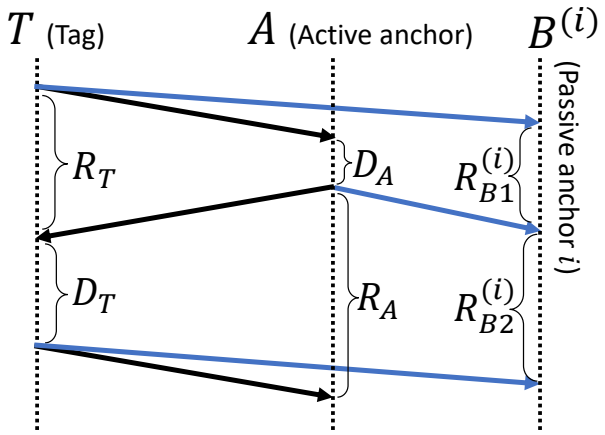


Fig. 2: The ranging protocol between active anchor and tag, overheard by a passive anchor.

we mitigate such range spoofing problem using collaboration from passively listening anchors. We first describe the passive ranging formulation, which allow the passive anchors to compute the tag's ToF through passive listening only and detect potential range spoofing through the collaboration of anchors. In case of spoofing, the passive anchors can still localize the attacker through our TDoA formulation.

A. UnSpoof-Passive ranging

Anchor A performs active ranging with a tag T using standard TWR. Assume all TWR messages and their contents between T and A are overheard by the set of passive anchors Bs. This message exchange is depicted in Fig. 2. At the end of this protocol, A determines the distance of the tag T from itself using (1).

Anchor B (used generically to mean any of the Bs anchors) passively overhears the message-exchange and records the time interval R_{B1} and R_{B2} between receiving consecutive messages (See Fig. 2). Anchor B can then compute the tag's ToF using the following UnSpoof-passive ranging formulation[1]:

$$\rho_{BT} = \rho_{AB} - \frac{D_T R_{B1} - R_{B2} R_T + R_A R_{B1} - R_{B2} D_A}{2\,(R_{B1} + R_{B2})} \quad (2)$$

To prove (2), we first express the relation between the measured time intervals shown in Fig. 2 and the ToFs as follows:

$$R_{B1} = \rho_{AT} + D_A + \rho_{AB} - \rho_{BT} \quad (3)$$
$$R_{B2} = \rho_{AT} + D_T + \rho_{BT} - \rho_{AB} \quad (4)$$

Following from $R_A = 2\rho_{AT} + D_T$, (4) can be rewritten as

$$R_A = R_{B2} + \rho_{AT} - \rho_{BT} + \rho_{AB} \quad (5)$$

[1]This is a variant of Eq. (3) in [8] where the role of A, B and T are switched. The detailed derivation was first shown in [8], and reproduced here with the appropriate changes for completeness.

Multiplying (3) and (5), it follows

$$\begin{aligned} &R_A R_{B1} - R_{B2} D_A \\ &= (R_{B2} + D_A + \rho_{AT} + \rho_{AB} - \rho_{BT})(\rho_{AT} + \rho_{AB} - \rho_{BT}) \\ &= (R_{B1} + R_{B2})(\rho_{AT} + \rho_{AB} - \rho_{BT}) \end{aligned}$$

$$\Rightarrow \rho_{AT} + \rho_{AB} - \rho_{BT} = \frac{R_A R_{B1} - R_{B2} D_A}{R_{B1} + R_{B2}} \quad (6)$$

Taking a similar approach, we can also obtain

$$\rho_{AT} - \rho_{AB} + \rho_{BT} = \frac{R_{B2} R_T - R_{B1} D_T}{R_{B1} + R_{B2}} \quad (7)$$

Subtracting (6) from (7), the passive ranging formulation can be expressed as:

$$\rho_{BT} = \rho_{AB} - \frac{D_T R_{B1} - R_{B2} R_T + R_A R_{B1} - R_{B2} D_A}{2\,(R_{B1} + R_{B2})}$$

In practical systems, the clock frequency may deviate from its correct value in an irregular fashion, introducing clock-drift error to ranging measurements [48]. Here, we show that the formulation in (1) is accurate despite clock imperfections. Denoting the clock drift rate of A, B and T to be δ_A, δ_B, and δ_T, the measured ToF by imperfect devices can be expressed as

$$\begin{aligned} \hat{\rho}_{BT} &= \rho_{AB} - \frac{(1+\delta_B)(1+\delta_T)(D_T R_{B1} - R_{B2} R_T)}{2(1+\delta_B)\,(R_{B1} + R_{B2})} \\ &\quad - \frac{(1+\delta_B)(1+\delta_A)(R_A R_{B1} - R_{B2} D_A)}{2(1+\delta_B)\,(R_{B1} + R_{B2})} \\ &= \rho_{AB} - \frac{(1+\delta_T)(D_T R_{B1} - R_{B2} R_T)}{2\,(R_{B1} + R_{B2})} \\ &\quad - \frac{(1+\delta_A)(R_A R_{B1} - R_{B2} D_A)}{2\,(R_{B1} + R_{B2})} \end{aligned}$$

The ToF error caused by clock drift is

$$\begin{aligned} &\hat{\rho}_{BT} - \rho_{BT} \\ &= -\frac{\delta_T (D_T R_{B1} - R_{B2} R_T)}{2\,(R_{B1} + R_{B2})} - \frac{\delta_A (R_A R_{B1} - R_{B2} D_A)}{2\,(R_{B1} + R_{B2})} \\ &= \frac{\delta_T}{2}(\rho_{AT} - \rho_{AB} + \rho_{BT}) - \frac{\delta_A}{2}(\rho_{AT} + \rho_{AB} - \rho_{BT}) \end{aligned}$$

Note that this quantity is on the sub-picosecond scale, which can be ignored for practical considerations. We experimentally verify this claim in Fig. 3 by comparing the UnSpoof-passive ranging against an existing passive TWR method [21]. Three Decawave DW1000 devices were set up to perform the message exchange shown in Fig. 2 continuously, while the response time D_A is reconfigured between trials. The measured time intervals were recorded and the passive range ρ_{BT} was computed using our formulation in (1) and the formulation found in [21] for comparison. Fig. 3 presents the cumulative distribution function (CDF) of the ranging error using the two different formulations. UnSpoof-passive ranging achieves 5cm standard deviation regardless of different system timing configuration, whereas the precision of the existing passive TWR method significantly vary depending on system timing configurations.

If the tag T is honest, and reports timestamps correctly, the obtained ρ_{BT} and ρ_{AT} will result in two circular locus

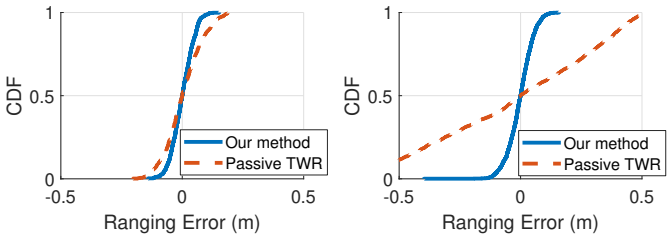


Fig. 3: Comparison between UnSpoof-passive ranging method in (2) and passive TWR [21]. (a) In fast ranging ($D_A \approx 5$ ms), our passive ranging method and passive TWR achieve similar precision. (b) In slow ranging ($D_A \approx 20$ ms), our passive ranging method retains high precision while passive TWR becomes significantly less precise.

centered at A and B respectively which intersect at the tag's location (and might also intersect at another reflection point). Adding one more passive anchor, it will be possible to unambiguously localize the tag T. We analyze localization accuracy for honest tags in our evaluation in Section IV-A.

B. Evidence of Spoofing

In the standard TWR system, a rogue tag can range with each anchor independently to obtain its location. Therefore, it can spoof all the ranging measurements independently by carefully crafting its reported timing information to each anchor, which in theory allows the spoofer to make itself appear to be anywhere it chooses. In UnSpoof-passive ranging, only one active TWR is performed, and the passive anchors calculate ToF using the same timing information the tag reported. Therefore, when the rogue tag spoofs the active TWR, all passive ranging are spoofed at the same time. Next, we prove that under UnSpoof, in practical systems, the amount of range reduction or enlargement is equal among all anchors (active and passive), and how this property can be used for spoofing detection.

1) Equal-spoofing Property: In a practical system, when a rogue tag spoofs the active TWR (1) by $\Delta\hat{\rho}_{AT}$ through manipulating R_T and D_T, all the passive ranges measured by the passive anchors using (2) are spoofed by approximately the same distance as the active range.

Proof: Assume the rogue tag spoofs R_T and D_T by $\Delta\hat{R}_T$ and $\Delta\hat{D}_T$, then the spoofed active range becomes

$$\begin{aligned}\hat{\rho}_{AT} &= \frac{(R_T+\Delta\hat{R}_T)R_A-(D_T+\Delta\hat{D}_T)D_A}{2(R_A+D_A)}\\ &= \frac{R_TR_A-D_TD_A}{2(R_A+D_A)}+\frac{\Delta\hat{R}_TR_A-\Delta\hat{D}_TD_A}{2(R_A+D_A)}\\ &= \rho_{AT}+\frac{\Delta\hat{R}_TR_A-\Delta\hat{D}_TD_A}{2(R_A+D_A)}\end{aligned}$$

Therefore, the spoofing distance is

$$\Delta\hat{\rho}_{AT}=\hat{\rho}_{AT}-\rho_{AT}=\frac{\Delta\hat{R}_TR_A-\Delta\hat{D}_TD_A}{2(R_A+D_A)}$$

.

Similarly, we can easily check that passive ranging using (2) is spoofed by

$$\Delta\hat{\rho}_{BT}=\hat{\rho}_{BT}-\rho_{BT}=\frac{\Delta\hat{R}_TR_{B2}-\Delta\hat{D}_TR_{B1}}{2(R_{B1}+R_{B2})}$$

.

Using the fact that $R_{B1}=\rho_{AT}+D_A+\rho_{AB}-\rho_{BT}$, $R_{B2}=\rho_{AT}+D_T+\rho_{BT}-\rho_{AB}$, and $R_A=D_T+2\rho_{AT}$, we can derive

$$\begin{aligned}\Delta\hat{\rho}_{BT}-\Delta\hat{\rho}_{AT} &= \frac{\Delta\hat{R}_T(R_{B2}-R_A)-\Delta\hat{D}_T(R_{B1}-D_A)}{2(R_{B1}+R_{B2})}\\ &= \frac{(\Delta\hat{R}_T+\Delta\hat{D}_T)(-\rho_{AT}+\rho_{BT}-\rho_{AB})}{2(R_{B1}+R_{B2})}\end{aligned}$$

In practical scenarios, $(\Delta\hat{R}_T+\Delta\hat{D}_T)$ and $(-\rho_{AT}+\rho_{BT}-\rho_{AB})$ are related to time-of-flight and thus should be on the scale of nano-seconds, i.e. 10^{-9} s, and $2(R_{B1}+R_{B2})$ contains radio response delays, which should be on the scale of milli-seconds [49], i.e. 10^{-3} s. Therefore, the difference between the spoofing distances $\Delta\hat{\rho}_{BT}-\Delta\hat{\rho}_{AT}$ should be on the scale of 10^{-15} s, which is equivalent to 10^{-7} meters in distance. This sub-micrometer difference is negligible in practical UWB localization systems and can be ignored. Therefore,

$$\Delta\hat{\rho}_{B^{(1)}T}\approx\Delta\hat{\rho}_{B^{(2)}T}\approx\ldots\approx\Delta\hat{\rho}_{B^{(i)}T}\approx\Delta\hat{\rho}_{AT}$$

■

The above property implies if the rogue tag spoofs the active TWR by X m, then the passive ranges measured by all the passive anchors are also spoofed by X m. This is a key difference from the standard as the standard TWR system allows the range of each anchor to be spoofed independently. This property is crucial for enabling spoofing detection by the localization solver.

2) Spoofing Detection Algorithm: Each range measurement geometrically defines a circular locus centered at the corresponding anchor. In an error-free TWR localization system, the circular loci defined by all the range measurements intersect at a single point, which is the tag's location. However, if the tag spoofs the reported timing information in an attempt to change its computed location, the circular locus generated by the passive anchors and the active anchor will not intersect at the same point.

Drawing on this observation, we design the following metric for detecting range spoofing using the inconsistencies in geometric relations. After one single TWR, the anchors obtain the measured distance vector

$$\hat{\mathbf{d}}=[\hat{d}_{AT},\hat{d}^{(1)}_{BT},\hat{d}^{(2)}_{BT}\ldots],$$

which defines the following system of equations

$$\begin{cases}||\mathbf{x}_A-\mathbf{x}||_2=\hat{d}_{AT}\\ ||\mathbf{x}^{(1)}_B-\mathbf{x}||_2=\hat{d}^{(1)}_{BT}\\ ||\mathbf{x}^{(2)}_B-\mathbf{x}||_2=\hat{d}^{(2)}_{BT}\\ \ldots\end{cases},\tag{8}$$

where $\mathbf{x}_A,\mathbf{x}^{(1)}_B,\ldots$ denote the coordinate of the anchors, $\mathbf{x}$ denotes the coordinate of the tag, and $||.||_2$ denotes the

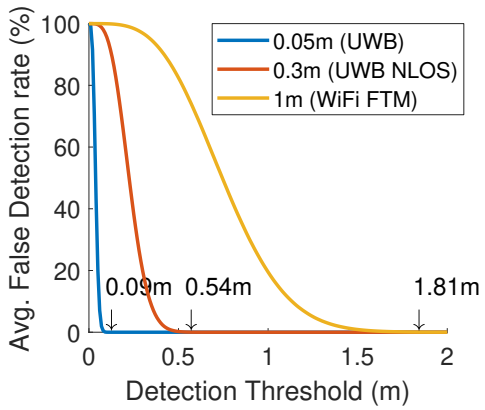


Fig. 4: Simulation result of the effect of detection threshold on the average false detection rate.

Euclidean distance between two points. (8) can be solved by a location solver to produce an estimate of the tag's location $\hat{\mathbf{x}}$ (in this work, we use the Levenberg-Marquardt nonlinear least square solver [50]). In the case of range spoofing, solving (8) results in large residual error since the range circles do not intersect at a single point. Therefore, the solver residual error can be used as a metric for spoofing detection. More specifically, we first compute the posterior distance vector $\tilde{\mathbf{d}} = [\tilde{d}_{AT}, \tilde{d}_{BT}^{(1)}, \tilde{d}_{BT}^{(2)}...] = [||\mathbf{x}_A, \hat{\mathbf{x}}||_2, ||\mathbf{x}_B^{(1)}, \hat{\mathbf{x}}||_2, ||\mathbf{x}_B^{(2)}, \hat{\mathbf{x}}||_2, ...]$, and then compute the root-mean-square error (RMSE) between $\hat{\mathbf{d}}$ and $\tilde{\mathbf{d}}$ as the detection metric for range spoofing. Finally, the residual-error-based detection metric is compared against a threshold–if the metric is larger than a certain threshold, spoofing is detected.

3) Choice of Detection Threshold: Of course, range spoofing is not the only cause for the solver residual-error. In any practical systems, the noisy ranging measurements also cause the range circles to not intersect at a single point. Therefore, the detection threshold has to be set as low as possible for high spoofing detection sensitivity, but also large enough to tolerate the noise of the ranging technology such that erroneous detection of spoofing almost never occurs. We investigate the false detection rate under various detection threshold values by Monte-Carlo simulation. As shown in Fig. 4, the false detection rate decreases when we increase the detection threshold. We should choose the smallest possible threshold value such that the false detection rate is nearly zero, which depends on the precision of the underlying ranging technology. For our UnSpoof-passive ranging scheme, the results in Fig. 3 shows ranging noise standard deviation of roughly 5cm, and Fig. 4 shows the false detection rate drops down to zero when the detection threshold is larger than 0.09m, or 9cm. In case different ranging noise levels are considered, such as UWB in non-line-of-sight (NLOS) environment or even WiFi Fine Timing Measurement (FTM) systems, an appropriate threshold should be chosen.

The spoofing detection process is summarized in Algorithm 1.

Algorithm 1 Spoofing Detection Algorithm.

Input: $\hat{\mathbf{d}} = [\hat{d}_{AT}, \hat{d}_{BT}^{(1)}, \hat{d}_{BT}^{(2)}...]$, d_{thresh}
1: $\hat{\mathbf{x}} \leftarrow$Localization solver for (8)
2: Compute posterior distance vector
$\tilde{\mathbf{d}} \leftarrow [||\mathbf{x}_A, \hat{\mathbf{x}}||_2, ||\mathbf{x}_B^{(1)}, \hat{\mathbf{x}}||_2, ||\mathbf{x}_B^{(2)}, \hat{\mathbf{x}}||_2, ...]$
3: Compute spoofing detection metric
$d_{metric} \leftarrow RMSE(\tilde{\mathbf{d}}, \hat{\mathbf{d}})$
4: Compare against detection threshold
if $d_{metric} > d_{thresh}$
return **TRUE**
else
return **FALSE**

C. Deterrence from Spoofing

A client will not perform spoofing if its location can still be identified, enabling the infrastructure to "catch" the spoofing node. This is the idea behind deterrence from spoofing. When a client indulges in range spoofing, the timing information reported by the tag is untrustworthy. We propose a modified formulation that can be used to compute the time-difference-of-arrival without R_T and D_T as follows[2]:

$$\rho_{AB} - \rho_{BT} = \frac{R_A R_{B1} - R_{B2} D_A}{R_A + D_A} - \rho_{AT} \tag{9}$$

Bringing the ρ_{AT} to the left hand side, we obtain an equation for the TDoA of signals sent by tag T.

$$T_{AB} = \rho_{BT} - \rho_{AT} = \rho_{AB} - \frac{R_A R_{B1} - R_{B2} D_A}{R_A + D_A} \tag{10}$$

There are three important properties of this TDoA formulation.

1) Spoofing-free Localization: Interestingly, the right hand side of (10) becomes independent of the time measurements reported by the tag and only relies on the time measurements of the trusted anchors. This observation *leads to the correct location of the tag, despite the tag trying to spoof its distance measurement*. Furthermore, since the spoofing tag can be located, it is possible to apprehend such a malicious actor, by calling in security, for example, in an industrial setting. This property leads to spoofing deterrence.

2) Wireless Synchronization: Traditional TDoA systems usually require wired clock synchronization among all the anchors [51]–[53], which could incur significant deployment or operational overhead. While these costs may not be prohibitive in industrial or commercial settings, and in fact UWB-based localization systems are much cheaper than alternative technologies, it is still desirable to develop simpler, more cost effective systems which function using only wireless message exchange, in lieu of wired synchronization. It can be observed that the UnSpoof-TDoA formulation only needs measurements of *time intervals* calculated by local clocks of the individual anchors. Therefore, it does not require any additional synchronization among the anchors, such as through routing the same clock to all anchors, which reduces the cost

[2]This is a variation from Eq. (2) in PnPLoc [8] by switching the role of A, B, and T, allowing an anchor to passively receive.

and operation overhead, and makes it suitable for scalable and ad-hoc applications.

3) Mitigation of Clock drift error: As we have shown, the reason accurate localization is possible in UnSpoof is because of robust mitigation of clock-drift effects. We now perform clock-drift analysis for UnSpoof-TDoA to show it is immune to such errors.

In practical systems, clock frequency deviates from the correct value, which causes the time measurement to be inaccurate. Denote the clock drift rate of A, B and T to be δ_A, δ_B, and δ_T. From (10), the measured TDoA $\hat{T}_{AB}$ is

$$\begin{aligned}\hat{T}_{AB} &= \rho_{AB} - \frac{\hat{R}_A\hat{R}_{B1} - \hat{R}_{B2}\hat{D}_A}{\hat{R}_A + \hat{D}_A} \\ &= \rho_{AB} - \frac{(1+\delta_A)(1+\delta_B)(R_AR_{B1} - R_{B2}D_A)}{(1+\delta_A)(R_A + D_A)} \\ &= \rho_{AB} - \frac{(1+\delta_B)(R_AR_{B1} - R_{B2}D_A)}{(R_A + D_A)}\end{aligned}$$

The error caused by the clock drift is

$$\begin{aligned}\hat{T}_{AB} - T_{AB} &= -\delta_B\frac{(R_AR_{B1} - R_{B2}D_A)}{(R_A + D_A)} \\ &= -\delta_B(\rho_{AB} - T_{AB})\end{aligned}$$

This error is on the scale of sub-picosecond, which is negligible. It can be similarly proved that (2) also nullifies the error caused by clock drift.

Overall, each of the equations we use in Section III are rooted in robust clock-drift independent formulations. Without these formulations, localization accuracy would suffer dramatically. Therefore, the formulations of calculating ToF and TDoA form the core mathematical backbone of this work.

D. Putting the System Together

We must answer two questions before we finalize the system design: (1) Why use ToF at all, if TDoA does not even require time stamps from the client? (2) How does the geometry of anchor placement affect the system?

1) Why ToF despite TDoA?: We have shown that a tag, after performing standard TWR with one active anchor, can be localized using either the ToF formulation in (2) or the TDoA formulation in (10). The key difference is that ToF is only accurate if the tag reports its timestamps honestly, while TDoA is accurate regardless of the integrity of the tag. It may seem that we can simply choose the TDoA formulation. Practically, every ranging measurement will have precision errors. We must therefore check if each scheme would perform acceptably in the face of precision errors that cause the distance estimate to be slightly incorrect.

TDoA-based localization which relies on overlapping hyperbolas has poor dilution of precision at the asymptotes, while ToF-based localization which depends on overlapping circles, has consistent accuracy within and around the convex hull defined by the anchors. Therefore, TDoA remains suitable only for coarse-grained localization of spoofing tags, whereas ToF should be used for more precise localization when the tag is honest. We investigate the accuracy of ToF and TDoA based localization experimentally in Section IV-A and Section IV-B.

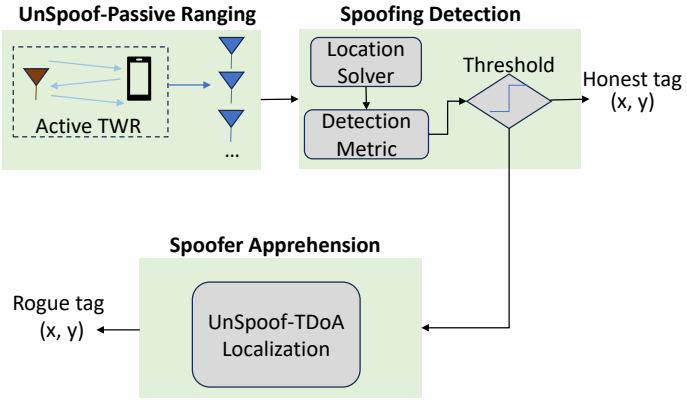


Fig. 5: The UnSpoof System

2) Geometry of Anchor Locations and Dilution of Precision: While ranging imprecision affects localization accuracy, the geometry of the placement of anchor nodes also directly affects the localization accuracy due to dilution of precision (DoP). Effects of high DoP are well-documented in GPS literature [54]. While the effect of DoP is accentuated for the short-range localization in our context [55], a full treatment of DoP is outside the scope of this paper. Further, the exact effect of DoP changes based on the geometry so much that we have taken the approach of just opening up the simulation we have built for that purpose and invite researchers to explore their own spaces through the simulator. We briefly explore the effects of different anchor configurations in Section IV-D.3.

3) Final System Design: Fig. 5 shows UnSpoof's complete system pipeline. UnSpoof has the ability to tell whether a tag is launching an internal-attack based spoofing using predetermined detection thresholds guided by the underlying ranging technology. Irrespective of spoofing or not, UnSpoof can always produce a reliable estimation of the tag's location (x, y). All of this is achieved with the tag performing the standard TWR with only one anchor at a time.

IV. Implementation and Evaluation

We have implemented UnSpoof on a set of 7 UWB DWM1000 devices. Each UWB device was controlled via a Cortex M0 microcontroller and ran our custom-built code. One of the UWB devices was setup as an active anchor and another was setup as a tag. The tag ranged (TWR) with a single active anchor only. Other 5 passive anchors were placed forming a hexagon with each side of 2m length covering a total area of $10.39\,m^2$. This setting allowed us to pre-measure the anchors' locations. Fig. 6 shows a photo of our overall setup, with a zoomed in version of the tag. The tag was placed at several locations in and around the convex hull created by the anchors. The anchors were plugged into an Intel i7 Dell laptop to capture all transmitted data for central processing. Localization was performed on the laptop using Matlab. To simulate range spoofing, the tag artificially modifies its timestamps to achieve specific range reduction or enlargement attack. As explained in Section III, this is done by simply perturbing D_T and R_T with appropriate amount corresponding to the specific spoofing distance. Next, we present the results from our experiments.

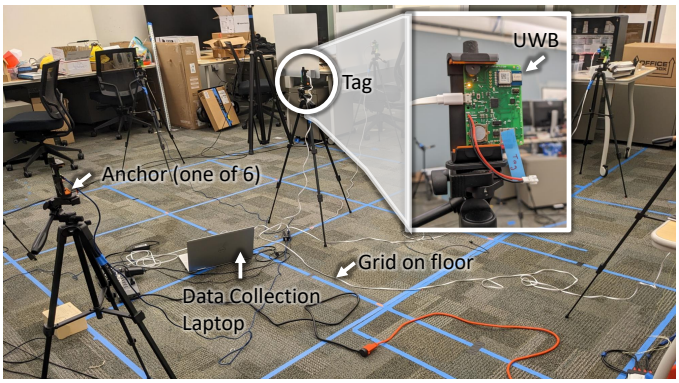


Fig. 6: Our practical implementation of UnSpoof in the lab space. A laptop captures data centrally for processing.

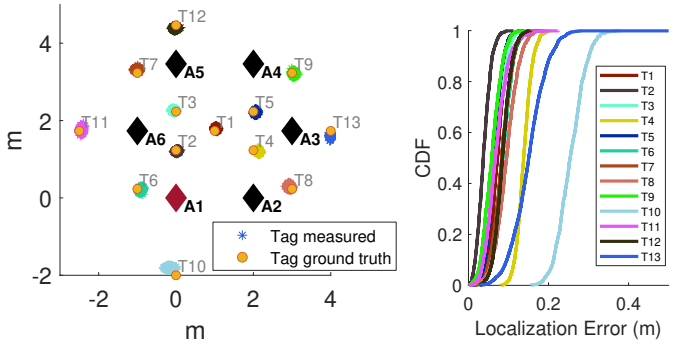


Fig. 7: Localization result using our passive ranging method in (2). (a) Scatterplot of measured tag location at 13 static locations. (b) CDF of localization error across 13 static tag locations. Both graphs are color-matched.

A. ToF based localization for honest tag

First, we report the localization results using the proposed UnSpoof-passive ranging formulation for an honest tag. Fig. 7 shows the CDFs for the localization result obtained from all the different tag locations. Only ToF information from UnSpoof-passive ranging was used in computing this information. It shows we can achieve around 20 cm localization error at 75^{th} percentile for most locations and 30 cm worst localization error at 75^{th} percentile.

B. TDoA based localization for malicious tag

The same experiment above is repeated but by using TDoA localization instead of ToF (shown in Fig. 8). While doing so, we do not use any information from inside the messages sent by the tag. We observe that the loss in localization accuracy is minimal in most cases. The localization is poorer where dilution of precision is a problem. Still, most tag locations show 50 cm localization error at 75^{th} percentile, enough for apprehending malicious users.

C. Effect of Number of Passive Anchors

In our previous experiments, we have used 5 passive anchors and one active anchor all arranged at the vertices of a regular hexagon. We now explore the effect of using only a subset of those anchors with a different anchor geometry.

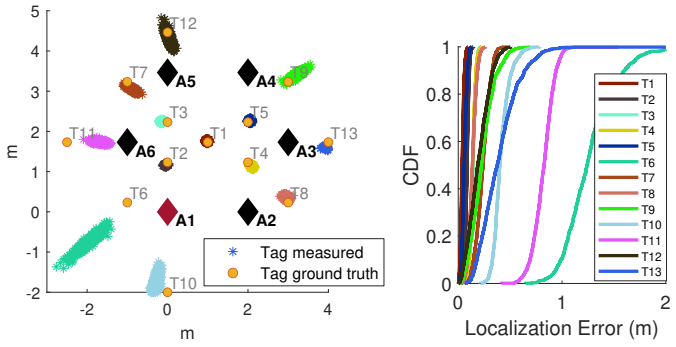


Fig. 8: Localization result using our passive TDoA ranging method in (10) for attacker apprehension. (a) Scatterplot of measured tag location at 13 static locations. (b) CDF of localization error across 13 static tag locations.

Fig. 9 shows that both ToF-based localization and TDoA-based localization suffer poorer localization precision when the number of passive anchors is decreased. This reduction in precision is smaller for ToF than for TDoA.

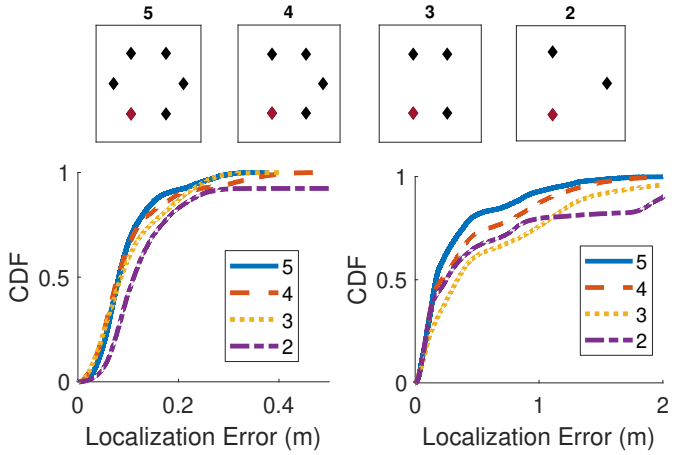


Fig. 9: Localization error CDF under varying number of passive anchors. (a) ToF based localization for honest tag. (b) TDoA based localization for malicious tag.

D. Spoofing Detection

First, we experimentally examine the effectiveness of spoofing detection with the same setup. Fig. 10 shows the spoofing detection rate versus the spoofing distance (negative for distance reduction attack, and positive for distance enlargement). For tag locations inside the convex hull of the anchors ($T1-5$), range reduction of 15 cm and range enlargement of 25 cm can be detected. For tag locations outside the convex hull of the anchors ($T6-13$), distance reduction can still be reliably detected if they try to pretend to be inside the convex hull. However, distance enlargement becomes more difficult to detect as some locations have poor DoP. This can be explained by Fig. 13c and Fig. 13d, where the tag is outside of the convex hull of the anchors. Fig. 13c shows the directions of expansion of the range circles in case of distance enlargement

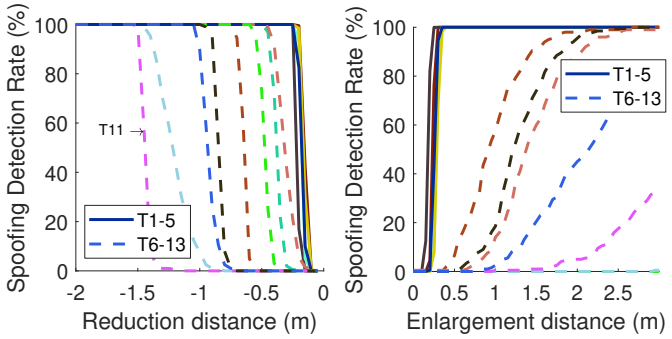


Fig. 10: The spoofing detection rate as a function of spoofing distance for all 13 tag locations. Range reduction is indicated by negative spoofing distance (x-axis), whereas positive spoofing distance indicate range enlargement. The continuous lines and dashed lines are for locations inside and outside the convex-hull created by the anchors respectively.

attacks, which are congruent. Therefore, as the range circles expand, they all expand towards the same direction such that a unique intersection can still be found (see Fig. 13d), making spoofing detection difficult. Interestingly, these cases correspond to regions of poor dilution of precision (DoP), at specific locations outside the convex hull as shown by the teal green streak at the left bottom corner in Fig. 8. However, in practice, this is unlikely to happen as anchors are supposed to cover the entire area of interest.

To better understand the effectiveness of the range spoofing method, we also investigate UnSpoof using Monte-Carlo simulation. First, we investigate the same anchor topology as our experiment where the 6 anchors form a regular hexagon. We generate 1600 test tag locations in a 10m-by-10m area. The ranging precision is assumed to match the experimental result in Fig. 3 (standard deviation=5cm). The spoofing is introduced by artificially adding the spoofing distance Δd to all range measurements.

1) Effect of detection threshold: We first investigate how the choice of detection threshold affects the system. In the case where the tag is honest (no spoofing), the choice of a larger detection threshold leads to lower false detection rate (see second row of Fig. 11), which is desired as honest tags wrongfully declared as spoofers can significantly reduce the usability of the system. On the other hand, as seen from the first and third row of Fig. 11, a larger detection threshold effectively shrinks the region where spoofing is detected. Therefore, it is important to choose the appropriate detection threshold to balance false detection rate and sensitivity.

2) Range reduction vs range enlargement: Is there any difference in detection of range reduction and range enlargement attacks? By comparing the first and third row of Fig. 11, we observe that spoofing detection is more sensitive to range reduction by $1\,m$ than range enlargement by the same amount. Within the anchors' convex hull, both range reduction and range enlargement can be detected with high confidence. However, outside of the anchors' convex hull, the area with high spoofing detection rate (bright yellow color) is noticeably larger for range reduction than range enlargement. This reconfirms the previous results in Fig. 10 and can similarly be explained with Fig. 13.

This suggests that in practice, (1) for a tag that's inside the anchors' convex hull, range spoofing (both range reduction and enlargement attacks) can be easily detected; (2) we can also reliably detect a rogue tag outside of the convex hull trying to appear to be inside the convex hull by launching range reduction attack; (3) the effectiveness of the spoofing detection is low if the tag is far outside the anchors' convex hull.

3) Anchor topology: In Fig. 12, we fix the detection threshold and examine the effect of different anchor topologies on spoofing detection. Similar to Topology A, Topology B and C also sees more effective detection for tag locations inside the anchors convex hull and detecting range reduction proves easier than detecting range enlargement. It can be observed that the shape of the region with high spoofing detection confidence depends on the anchor topology. In Topology B and C, the anchors are more spread out, which results in larger high-confidence spoofing detection regions. This suggests that in practice when deploying the anchors, the anchor topology should surround the region in which secure localization needs to be carried out.

V. Discussion and Concluding Remarks

Spoofing evident or spoofing free localization might usher in a new wave of trustworthy applications using UWB and indoor localization in general (the techniques we mention here should also work for WiFi FTM, for example). We have shown in UnSpoof that it is possible to provide such a capability while relying on a very small number of message exchanges. We have demonstrated the capability through real-world experiments using a set of real UWB devices. Our experiments are performed in controlled lab settings. Of course, testing over longer distances and NLOS measurements would be required to transition UnSpoof into a product. However, our novel formulation for passive ToF, passive TDoA, and spoofing detection is expected to become a foundational technology for future localization work, and those that use trustworthy localization as a primitive for enabling other applications. We have open sourced our simulation in the following repository to facilitate future research in trustworthy localization by other researchers: `https://github.com/haigeandychen/UnSpoof-Simulation`.

A. Enabling New Applications

We envision a spoofing-free localization solution will enable several applications:

1) Seamless Access Control: UWB localization can be used for granting clients access to physical spaces with physical proximity seamlessly, with potential applications in vehicle entry, smart locks in home automation, or secure facilities. For example, access control ID cards in factories could use UWB localization, providing both access to the user as well as traceable activity monitoring for compliance, auditing, and safety and security purposes. The potential threat model that

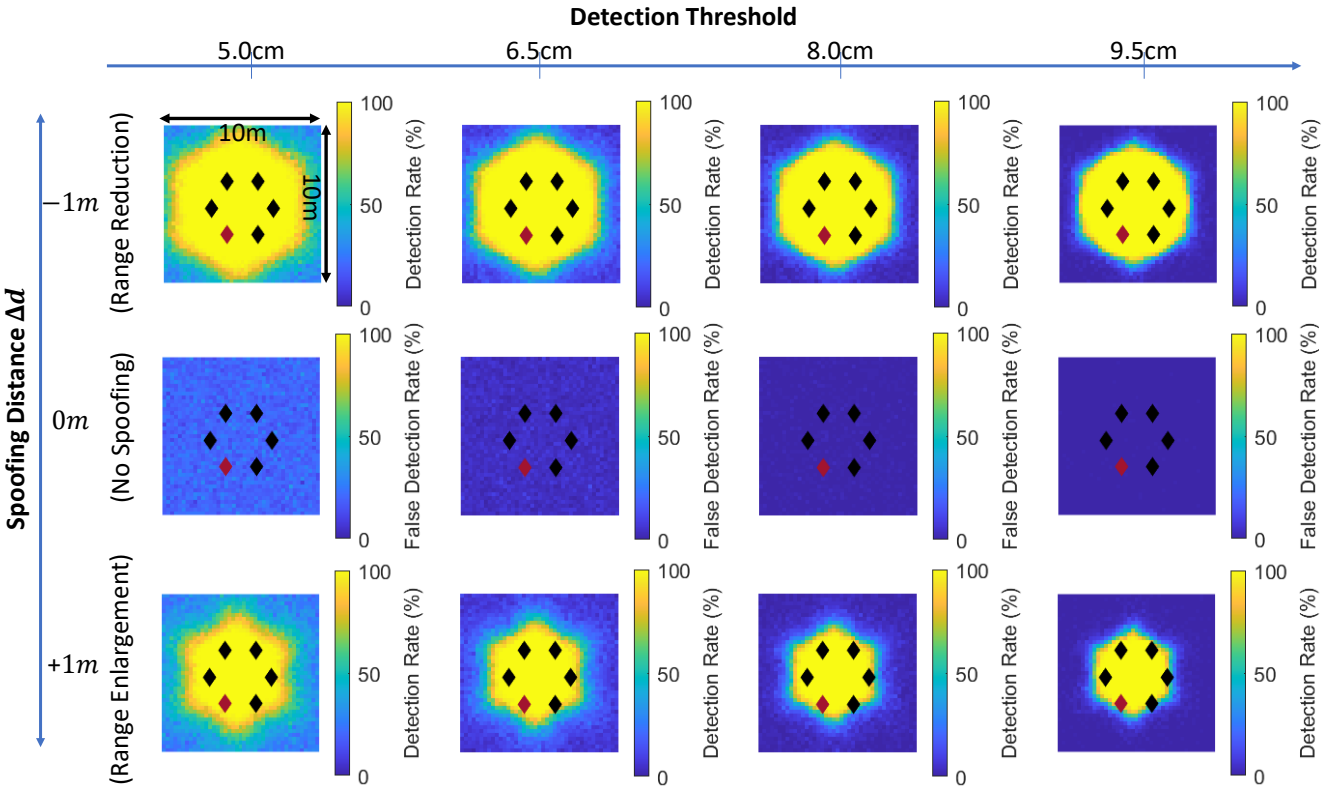


Fig. 11: Simulation of spoofing detection rate heatmap under different choice of spoofing detection threshold and spoofing distance. The active and passive anchors are shown as red and black diamond shapes. A high spoofing detection rate (close to 100%) is represented by brighter color in the heatmap.

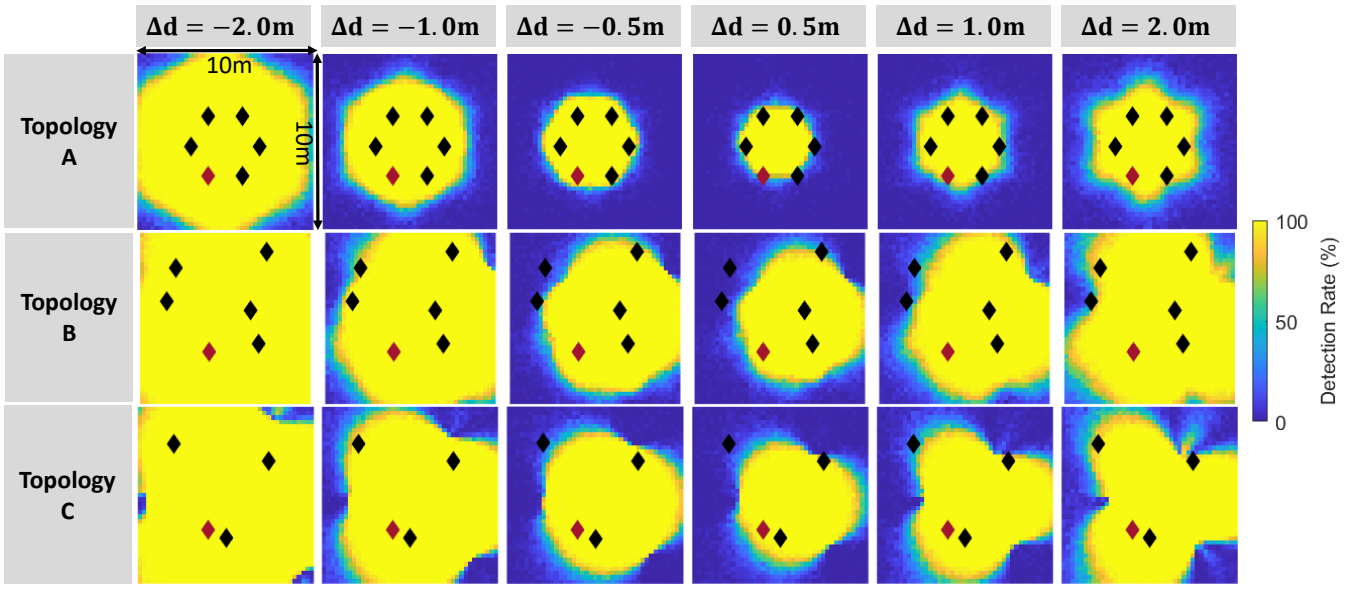
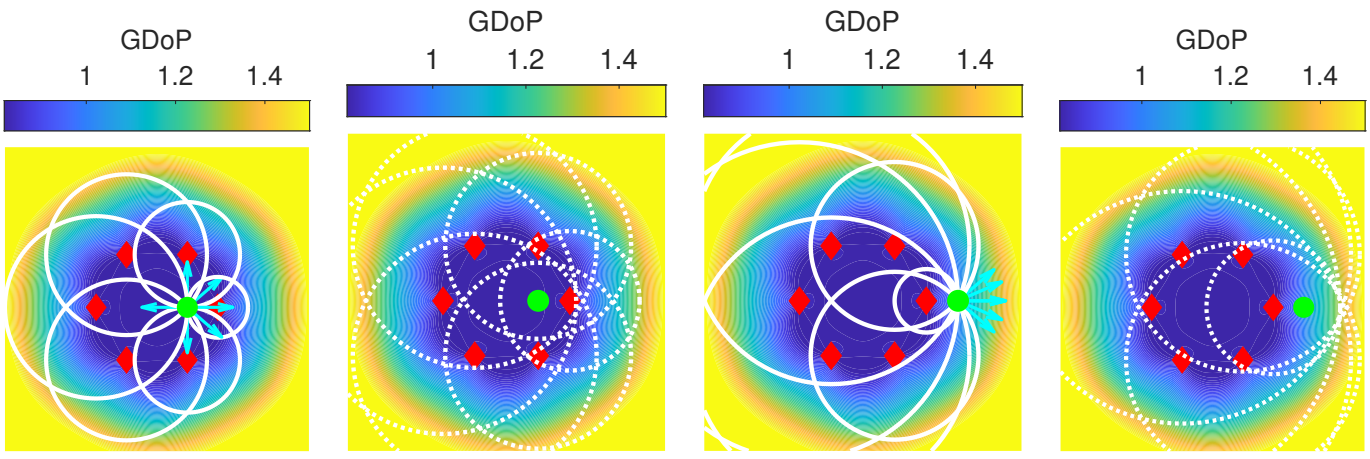


Fig. 12: Simulation of spoofing detection rate vs spoofing distance under three different anchor topologies.

we wish to prevent in UnSpoof is when a malicious user tampers with their UWB-based ID card changing the timestamps in UWB messages sent by their ID card. Such tampering may allow the malicious user to wander to places in the factory building without leaving a trace of their whereabouts, since the infrastructure might wrongly infer the malicious user's location from the tampered timestamps.

2) Location-based content delivery: Many scenarios require information to be location-sensitive, e.g. concerts, sporting events, or museums where only legitimate patrons inside the venue may access certain service, which can be enabled by spoofing-free localization. An example application is in a hos-



(a) (b) (c) (d)

Fig. 13: Effect of DoP on spoofing detection. The anchor locations are shown as red diamond. The tag location is shown as green circle. The solid and dotted white lines show the range circles that correspond to real and spoofed distances respectively. The arrows in (a) and (c) show the direction of expansion of the range circles in case of range spoofing attacks. GDoP is shown as the color of the underlying heatmap. (a) When the tag is inside the convex hull of the anchors (low DoP), the range circles expand in incoherent and opposite directions in case of spoofing. (b) The resulting range circles under spoofing do not intersect at a single point, and spoofing can be detected. (c) When the tag is outside the convex hull of the anchors (high DoP), the range circles expand in similar directions in case of spoofing. (d) The resulting range circles under spoofing still intersect at roughly a single point, thus making spoofing detection more difficult.

pital setting; data can be made freely available to doctors while present in a patient's room, but wiped off and inaccessible outside.

3) Proof-of-presence: UnSpoof can enable certain applications that require proof of physical presence for legal or certification purposes, such as verified package delivery, attendance checking, and verified returns (of book, parcel, or vehicle to a designated place for example). In all of the above applications, location spoofing is highly motivated as the spoofer can almost always benefit from such attack. Our proposed system UnSpoof takes a crucial step towards making spoofing-free localization and its applications a reality.

B. Potential Attacks on UnSpoof

UnSpoof's capabilities are limited to detecting spoofed timing reports. We point out a few conditions under which UnSpoof will show sub-optimal performance.

1) Multi-antenna Client—Different messages to different anchors: If the client device has multiple antennas, it could simultaneously send different messages in different directions. This will result in the passive anchors all receiving different timing information from inside the messages and infer a lack of spoofing. To prevent such an attack, UnSpoof passive anchors should also pass along the actual timing information they read from inside the message. At the active anchor, if this information varies from what it received, a spoofing attack must be inferred.

2) Multi-antenna Client—Different delays to different anchors: Another method of cheating despite the presence of UnSpoof for a multi-antenna client is to delay the transmission of signals in different directions. This results in incorrect timing calculations at the anchors and such a sophisticated attack might succeed. However, slightly delayed signals may be identified using the rich channel impulse response thatUWB can obtain, due to side lobe emissions by practical multi-antenna systems. We have not explored this possibility in UnSpoof and leave it to future work.

3) Compromised Passive Anchors: If the passive anchors are compromised, then UnSpoof cannot function. However, such an attack is relatively easy to stop by encrypting messages between the passive anchors and the active anchor. Since the encryption key will only be known to the authentic anchors, it is not possible for malicious new anchors to be introduced in the system.

C. Systems Considerations

1) Battery Life: Passive anchors must always listen for any UWB communication and report the messages they receive to the active anchor. Since wireless reception cannot be duty cycled, the passive anchors expend significantly more energy than the client device. However, we expect that the anchors, both active and passive, will be mains powered and battery-life is not a consideration for those anchors. We will leave exploration of a low-power alternative for future work.

2) Processing Load: UnSpoof uses a simple solver for ToF based localization of honest tags. The processing load is taken up by the active anchor, using all the information it receives from other passive anchors. However, if it detects inconsistencies, the active anchor must perform a second localization based on TDoA which adds to the processing load at the active anchor. However, this increased load is the price the active node pays to apprehend the spoofing tag. If the active node decides to only detect spoofing tags and not act

on it to find such a tag's location, then the active node would not experience any additional processing load.

3) Maximizing Update Rate and Number of Supported Client: UnSpoof already improves the possible update rate since it only ranges with a single active tag. One way to improve update rate is through sending the packet information from the passive anchors to the active anchors using a non-UWB wireless technology, such as Wi-Fi. This prevents wasting UWB air-time and allows a faster update of location information. When there are more than one clients, they must take turns for transmitting, reducing effective update rate for each client. A multi-client collaborative pipelined two-way ranging scheme as used in [55] or in [56] can be employed if the clients can agree on an ordering of POLL messages.

4) Performance in non-line of sight conditions: Non-line of sight conditions can degrade the precision of TWR ranging measurements. Such conditions can affect both the active anchor as well as the passive anchors. It will be helpful to add a confidence metric to each reported measurement by the passive anchors. This confidence metric can be based on any of the LOS-NLOS detection mechanisms that exist in literature, such as those employed by [57]. Employing such a metric is outside of the scope of this paper, and therefore we leave it to future work.

In conclusion, UnSpoof provides a novel approach to tackle location spoofing attacks launched through malicious manipulation of reported timestamps by clients. We expect UnSpoof to become standard practice in UWB localization in the future. It will enable new applications and strengthen existing ones, significantly contributing to the current literature on secure UWB ranging.

REFERENCES

[1] Locatify, "What is the new Apple U1 chip, and why is it important?." https://bit.ly/413oHQe, 2020.

[2] K. Vyas, "Google has added an Ultra-wideband (UWB) API in Android." https://www.xda-developers.com/google-adding-ultra-wideband-uwb-api-android/, 2021.

[3] K. Kim, "Samsung Expects UWB To Be One of the Next Big Wireless Technologies." https://bit.ly/412xLVC, 2020.

[4] S. Jogi, "NXP Continues to Advance UWB, Taking Accuracy to mm Level." https://bit.ly/47E4gvO, 2023.

[5] D. Neirynck, E. Luk, and M. McLaughlin, "An alternative double-sided two-way ranging method," *2016 13th Workshop on Positioning, Navigation and Communications (WPNC)*, pp. 1–4, 10 2016.

[6] L. S. Committee, *IEEE Standard for Low-Rate Wireless Networks. Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques (IEEE Std 802.15.4z)*, vol. 2020. 2020.

[7] S. IEEE, *IEEE Standard for Local and metropolitan area networks — Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*, vol. 2011. 2011.

[8] H. Chen and A. Dhekne, "PnPLoc: UWB based plug & play indoor localization," in *2022 IEEE 12th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 1–8, 2022.

[9] IEEE802.15.4z, "IEEE Standard for Low-Rate Wireless Networks–Amendment 1: Enhanced Ultra Wideband (UWB) Physical Layers (PHYs) and Associated Ranging Techniques," *IEEE Std 802.15.4z-2020 (Amendment to IEEE Std 802.15.4-2020)*, pp. 1–174, 2020.

[10] H. Chen and A. Dhekne, "UnSpoof: Distance spoofing-evident localization using UWB," in *2023 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2023.

[11] F. Zafari, A. Gkelias, and K. K. Leung, "A survey of indoor localization systems and technologies," *IEEE Communications Surveys Tutorials*, vol. 21, no. 3, pp. 2568–2599, 2019.

[12] A. Alarifi, A. Al-Salman, M. Alsaleh, A. Alnafessah, S. Al-Hadhrami, M. A. Al-Ammar, and H. S. Al-Khalifa, "Ultra wideband indoor positioning technologies: Analysis and recent advances," *Sensors*, vol. 16, no. 5, 2016.

[13] D. Coppens, A. Shahid, S. Lemey, B. Van Herbruggen, C. Marshall, and E. De Poorter, "An overview of uwb standards and organizations (ieee 802.15.4, fira, apple): Interoperability aspects and future research directions," *IEEE Access*, vol. 10, pp. 70219–70241, 2022.

[14] A. Alarifi, A. Al-Salman, M. Alsaleh, A. Alnafessah, S. Al-Hadhrami, M. A. Al-Ammar, and H. S. Al-Khalifa, "Ultra wideband indoor positioning technologies: Analysis and recent advances," *Sensors*, vol. 16, no. 5, 2016.

[15] M. Zhao, T. Chang, A. Arun, R. Ayyalasomayajula, C. Zhang, and D. Bharadia, "Uloc: Low-power, scalable and cm-accurate UWB-tag localization and tracking for indoor applications," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 5, sep 2021.

[16] N. Smaoui, M. Heydariaan, and O. Gnawail, "Single-antenna aoa estimation with UWB radios," in *2021 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, 2021.

[17] M. Heydariaan, H. Dabirian, and O. Gnawali, "Anguloc: Concurrent angle of arrival estimation for indoor localization with UWB radios," in *2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, pp. 112–119, 2020.

[18] G. Caso, M. T. P. Le, L. De Nardis, and M.-G. Di Benedetto, "Performance comparison of WiFi and UWB fingerprinting indoor positioning systems," *Technologies*, vol. 6, no. 1, 2018.

[19] W. Vinicchayakul and S. Promwong, "Improvement of fingerprinting technique for UWB indoor localization," in *The 4th Joint International Conference on Information and Communication Technology, Electronic and Electrical Engineering (JICTEE)*, pp. 1–5, 2014.

[20] P. Corbalán and G. P. Picco, "Ultra-wideband concurrent ranging," *ACM Trans. Sen. Netw.*, vol. 16, sep 2020.

[21] T. Laadung, S. Ulp, M. M. Alam, and Y. L. Moullec, "Active-passive two-way ranging using UWB," *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pp. 1–5, 12 2020.

[22] K. A. Horvath, G. Ill, and A. Milankovich, "Passive extended double-sided two-way ranging with alternative calculation," *2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband, ICUWB 2017 - Proceedings*, vol. 2018-Janua, pp. 1–5, 2018.

[23] B. Großwindhager, M. Stocker, M. Rath, C. A. Boano, and K. Römer, "Snaploc: An ultra-fast UWB-based indoor localization system for an unlimited number of tags," in *2019 18th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pp. 61–72, 2019.

[24] J. Tiemann, F. Eckermann, and C. Wietfeld, "Atlas - an open-source tdoa-based ultra-wideband localization system," in *2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 1–6, 2016.

[25] A. Ledergerber, M. Hamer, and R. D'Andrea, "A robot self-localization system using one-way ultra-wideband communication," vol. 2015-Decem, pp. 3131–3137, IEEE, 9 2015.

[26] A. Arun, S. Saruwatari, S. Shah, and D. Bharadia, "Xrloc: Accurate uwb localization for XR systems," 2023.

[27] A. Biri, N. Jackson, L. Thiele, P. Pannuto, and P. Dutta, "Socitrack: Infrastructure-free interaction tracking through mobile sensor networks," in *Proceedings of the 26th Annual International Conference on Mobile Computing and Networking*, MobiCom '20, (New York, NY, USA), Association for Computing Machinery, 2020.

[28] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 829–835, April 2006.

[29] P. McWilliams, "Uwb spreads its wings for secure keyless access." https://tinyurl.com/5drmxtda, 2021.

[30] P. Zhang, S. G. Nagarajan, and I. Nevat, "Secure Location of Things (SLOT): Mitigating Localization Spoofing Attacks in the Internet of Things," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 2199–2206, 2017.

[31] M. Shariat and W. Kastner, "Authenticated UWB-based positioning of passive drones," in *2023 IEEE 19th International Conference on Factory Communication Systems (WFCS)*, pp. 1–8, 2023.

[32] K. B. Rasmussen and S. Čapkun, "Location privacy of distance bounding protocols," in *Proceedings of the 15th ACM Conference on Com-*

puter and Communications Security, CCS '08, (New York, NY, USA), p. 149–160, Association for Computing Machinery, 2008.
[33] Y. Xue, W. Su, H. Wang, D. Yang, and Y. Jiang, "Deeptal: Deep learning for tdoa-based asynchronous localization security with measurement error and missing data," *IEEE Access*, vol. 7, pp. 122492–122502, 2019.
[34] Y. Zhang, W. Liu, Y. Fang, and D. Wu, "Secure localization and authentication in ultra-wideband sensor networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 4, pp. 829–835, 2006.
[35] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 221–232, Feb 2006.
[36] M. Stocker, B. Großwindhager, C. A. Boano, and K. Römer, "Towards Secure and Scalable UWB-based Positioning Systems," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 247–255, 2020.
[37] M. Singh, P. Leu, A. Abdou, and S. Capkun, "UWB-ED: Distance enlargement attack detection in Ultra-Wideband," in *28th USENIX Security Symposium (USENIX Security 19)*, (Santa Clara, CA), pp. 73–88, USENIX Association, Aug. 2019.
[38] P. Leu, G. Camurati, A. Heinrich, M. Roeschlin, C. Anliker, M. Hollick, S. Capkun, and J. Classen, "Ghost peak: Practical distance reduction attacks against HRP UWB ranging," in *31st USENIX Security Symposium (USENIX Security 22)*, (Boston, MA), pp. 1343–1359, USENIX Association, Aug. 2022.
[39] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec, "On Secure and Precise IR-UWB Ranging," *IEEE Transactions on Wireless Communications*, vol. 11, no. 3, pp. 1087–1099, 2012.
[40] P. Perazzo, L. Taponecco, A. A. D'amico, and G. Dini, "Secure Positioning in Wireless Sensor Networks through Enlargement Miscontrol Detection," *ACM Trans. Sen. Netw.*, vol. 12, sep 2016.
[41] Y. Wang, X. Ma, and G. Leus, "An UWB ranging-based localization strategy with internal attack immunity," in *2010 IEEE International Conference on Ultra-Wideband*, vol. 2, pp. 1–4, 2010.
[42] B. Pestourie, *UWB based Secure Ranging and Localization*. PhD thesis, 2020. Thèse de doctorat dirigée par Beroulle, Vincent et Fourty, Nicolas Nanoélectronique et nanotechnologie Université Grenoble Alpes 2020.
[43] Y. Wang, X. Ma, and G. Leus, "Robust Time-Based Localization for Asynchronous Networks," *IEEE Transactions on Signal Processing*, vol. 59, pp. 4397–4410, Sep. 2011.
[44] S. Capkun, K. 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, 2008.
[45] N. O. Tippenhauer and S. Capkun, "UWB-based secure ranging and localization," *Technical Report/ETH Zurich, Department of Computer Science*, vol. 586, 2012.
[46] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "UWB Rapid-Bit-Exchange System for Distance Bounding," in *Proceedings of the 8th ACM Conference on Security Privacy in Wireless and Mobile Networks*, WiSec '15, (New York, NY, USA), Association for Computing Machinery, 2015.
[47] K. A. Horvath, G. Ill, and A. Milankovich, "Passive Extended Double-Sided Two-Tay Ranging Algorithm for UWB Positioning," *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, pp. 482–487, 7 2017.
[48] H. Chen and A. Dhekne, "A metric for quantifying uwb ranging error due to clock drifts," in *2022 IEEE 12th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 1–8, 2022.
[49] M. von Tschirschnitz, M. Wagner, M.-O. Pahl, and G. Carle, "Clock error analysis of common time of flight based positioning methods," *2019 International Conference on Indoor Positioning and Indoor Navigation, IPIN 2019*, 9 2019.
[50] J. J. Moré, "The levenberg-marquardt algorithm: Implementation and theory," in *Numerical Analysis* (G. A. Watson, ed.), (Berlin, Heidelberg), pp. 105–116, Springer Berlin Heidelberg, 1978.
[51] "Zebra uwb technology product datasheet." `https://bit.ly/3Fji5Bs`, 2018.
[52] V. Djaja-Josko and J. Kolakowski, "A new transmission scheme for wireless synchronization and clock errors reduction in uwb positioning system," in *2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 1–6, 2016.
[53] J. Tiemann, F. Eckermann, and C. Wietfeld, "ATLAS - an open-source TDOA-based Ultra-wideband localization system," in *2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pp. 1–6, 2016.
[54] R. B. Langley, "Dilution of Precision," *GPS World*, vol. 10, pp. 52–59, 1999.
[55] A. Dhekne, U. J. Ravaioli, and R. R. Choudhury, "P2ploc: Peer-to-peer localization of fast-moving entities," *Computer*, vol. 51, no. 10, pp. 94–98, 2018.
[56] A. Dhekne, A. Chakraborty, K. Sundaresan, and S. Rangarajan, "TrackIO: Tracking first responders Inside-Out," in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI 19)*, (Boston, MA), pp. 751–764, USENIX Association, Feb. 2019.
[57] Y. Cao, A. Dhekne, and M. Ammar, "6Fit-A-Part: A Protocol for Physical Distancing on a Custom Wearable Device," in *2020 IEEE 28th International Conference on Network Protocols (ICNP)*, pp. 1–12, IEEE, 2020.

Haige Chen (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering in 2019 from the University of Illinois Urbana-Champaign, USA. He received the M.S. degree in electrical and computer engineering in 2021 from Georgia Institute of Technology, USA. And he is currently working towards the Ph.D. degree in electrical and computer engineering at Georgia Institute of Technology, USA.

His research interests are indoor localization, wireless sensing and communication, and IoT.

Ashutosh Dhekne (Member, IEEE) received his Ph.D. from the University of Illinois at Urbana-Champaign in 2019. He is currently an Assistant Professor at the School of Computer Science at Georgia Institute of Technology, USA where is is currently a BBISS Faculty Fellow. He is the recipient of the NSF CAREER award, Richard T. Cheng Fellowship, and the NTSE Scholarship. His research interests are mobile computing, IoT, and wireless-networking, wireless-localization, and wireless-sensing.