UnSpoof: Distance Spoofing-Evident Localization using UWB

Haige Chen
Georgia Institute of Technology
Atlanta, USA
hchen425@gatech.edu

Ashutosh Dhekne
Georgia Institute of Technology
Atlanta, USA
dhekne@gatech.edu, ORCiD 0000-0001-6272-8521

***Abstract*—This paper presents UnSpoof, a UWB localization system that can detect and localize distance-spoofing tags with several collaborative passively-receiving anchors. We propose novel formulations that enable passively-receiving anchors to deduce their time-of-arrival (ToA) and time-difference-of-arrival (TDoA) just by overhearing standard two-way ranging (TWR) messages between the tag and one active anchor. Our ToA 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 spoof-free localization, which can be used to track down and apprehend a malicious tag. Our experimental evaluation shows 30 cm 75^{th} percentile error for ToA-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.**

***Index Terms*—Secure UWB Localization, Distance Spoofing, Active-Passive Localization, TWR+TDoA localization**

I. Introduction

This paper presents a rather surprising result: it is possible for a set of fixed collaborating ultra-wideband (UWB) anchors to (i) obtain accurate location of a UWB client device, (ii) *detect* if the UWB client is trying to spoof the distance measurement by lying about its timestamps, and (iii) obtain approximate location of a spoofing device *without* trusting any timestamps in the spoofing device's messages, all *using just a single two-way ranging measurement* between the client and one active anchor so long as other passively listening anchors collaborate with the active anchor. We show that these properties are upheld not just inside the convex hull described by the anchors, but also, to a certain degree, outside the convex hull. We first 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.

A key reason that all of the above properties can be achieved is due 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 [3] by shunning the previous averaging formulation in the IEEE802.15.4a standard [6] for localization. In a completely different context, a similar

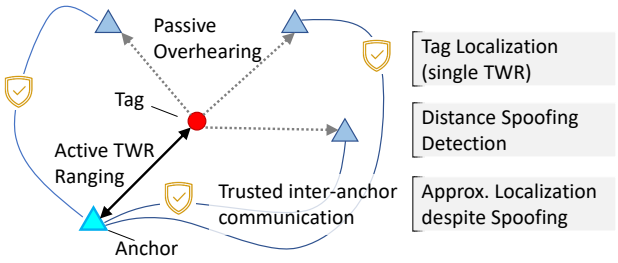


Fig. 1: UnSpoof setup includes a single active ranging tag-anchor pair. Other passively listening anchors share their observations collaboratively, which enables tag localization, detection of distance spoofing by tag, and approximate localization despite spoofing.

improvement in the formulation of time-difference-of-arrival (TDoA) was presented in our IPIN 2022 paper in a system called PnPLoc [2]. While the TDoA derivation in PnPLoc pertained to a scalable privacy preserving system for a client UWB device to obtain its own location, the context of the current work is completely different. Here the infrastructure anchors wish to obtain the location of a client UWB. This is a common use-case for localization in industrial IoT, for example, where the company centrally monitors the location of all its assets inside the building.

It is natural to wonder: *is there any need to have secure localization at all?* We contend that one of the reasons indoor localization has remained simply a support service or a good-to-have feature is because it's validity is not provable. If it was possible to prove that a UWB tag was indeed at a certain location, a plethora of new applications could be enabled. This includes, for example, enabling physical access control in companies via UWB smartphones, 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 accurate timestamps, verifiable signatures from the infrastructure anchors, etc.).

We now introduce UnSpoof (depicted in Figure 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 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 [7], 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 time-difference-of-arrival (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. To the best of our knowledge, no other system can achieve this set of attributes. Next, we will briefly dwell on the limited related work on this topic.

II. Related Work

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 modifies the received physical wireless pulse [10], [15], or spoof distance measurements where a participating tag maliciously alters timing information [17]. 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 [14], [17]. Others have previously found, similar to our results, that if overhearing trusted anchors exist, such spoofing can be *detected* [14], [17]. However, they focus on a single sided ranging protocol, which is quite inaccurate in face of clock drifts. In [13], the authors proposed the Verifiable Multilateration method based on distance bounding, which typically requires special hardware [16]. We show that spoofing detection is possible when the system simply uses the latest IEEE 802.15.4z [7] 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 [2], 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 actually possible to detect spoofing outside the convex hull when using our ToA based validation. To the best of our knowledge, no other system has shown these properties. It's worth noting that different from [4], [5], which also achieve passive ranging by overhearing anchors, our method can extract ToA and TDoA at the same time balancing accuracy for honest tags and ability to apprehend dishonest ones.

III. UnSpoof System Design for Practitioners

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 [12]:

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

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. In TWR, a malicious tag can spoof the measurement of ρ_{AT} simply by reporting untruthful timing information R_T and D_T. It's 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, we mitigate such range spoofing problem using collaborations from passively listening anchors. We first describe the passive ranging formulation, which allow the passive anchors to compute the tag's ToA 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.

UnSpoof-Passive ranging: 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 Figure 2. At the end of this protocol, A determines the distance of the tag T from itself using Equation 1.

Anchor B (used generically to mean any of the Bs anchors) passively overhears the message-exchange and calculates its own estimate of the $B-T$ distance denoted as ρ_{BT} using the below formulation[1]:

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

[1]This is a variant of Equation 3 in [1] where the role of A, B and T are switched. The detailed derivation can be found in [1].

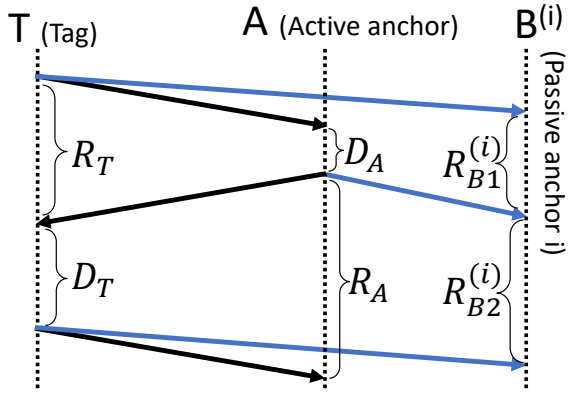


Fig. 2: The ranging protocol between active anchor and tag, overheard by a passive anchor.

where ρ_{AB} denotes the known distance between the active and passive anchors.

If the tag T is honest, and reports timestamps correctly, the obtained ρ_{BT} and ρ_{AT} will result in two circular locus 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. Figure 3a shows the case of honest tag being fully localized using one active and several passive anchors.

However, if T spoofs the reported timing information in an attempt to change its computed location, the circular locus generated by the passive anchors B_i and B_j, and the active anchor A will not intersect uniquely. Location cannot be determined using ToA, but such an incidence indicates likely spoofing. More specifically, it's easy to see range reduction attack on ρ_{AT} by lowering R_T and increasing D_T also cause ρ_{BT} to decrease, and vice versa. Figure 3b shows the case of a tag spoofing the distance measurement that results in non-intersecting circular locus which results in the inability to resolve a location.

Spoofing detection: 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 $\hat{\mathbf{d}} = (\hat{d}_{AT}, \hat{d}_{BT}^{(1)}, \hat{d}_{BT}^{(2)}...)$, which is supplied to 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 [11]). From $\hat{\mathbf{x}}$, we can compute the predicted distance vector $\tilde{\mathbf{d}} = (\tilde{d}_{AT}, \tilde{d}_{BT}^{(1)}, \tilde{d}_{BT}^{(2)}...) = (dist(A, \hat{\mathbf{x}}), dist(B^{(1)}, \hat{\mathbf{x}}), dist(B^{(2)}, \hat{\mathbf{x}}), ...)$. In case of range spoofing, the range circles defined by $\hat{\mathbf{d}} = (\hat{d}_{AT}, \hat{d}_{BT}^{(1)}, \hat{d}_{BT}^{(2)}...)$ actually do not intersect at $\hat{\mathbf{x}}$, and $\hat{\mathbf{d}}$ disagrees with $\tilde{\mathbf{d}}$. Here, we use the root-mean-square error (RMSE) between $\hat{\mathbf{d}}$ and $\tilde{\mathbf{d}}$ as the detection metric for range spoofing, with thresholds set to appropriately compensate for the typical localization error tolerance of the ranging technology ($20\,cm$ for UWB).

UnSpoof-TDoA: In case of 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]:

$$\rho_{AB} - \rho_{BT} = \frac{R_A R_{B1} - R_{B2} D_A}{R_A + D_A} - \rho_{AT} \tag{3}$$

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

$$T_{AB} = \rho_{BT} - \rho_{AT} = \rho_{AB} - \frac{R_A R_{B1} - R_{B2} D_A}{R_A + D_A} \tag{4}$$

Interestingly, the right hand side 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. It's worth noting that this TDoA formulation does not require any synchronization among the anchors, which makes it suitable for scalable and ad-hoc applications.

A. Practical Considerations

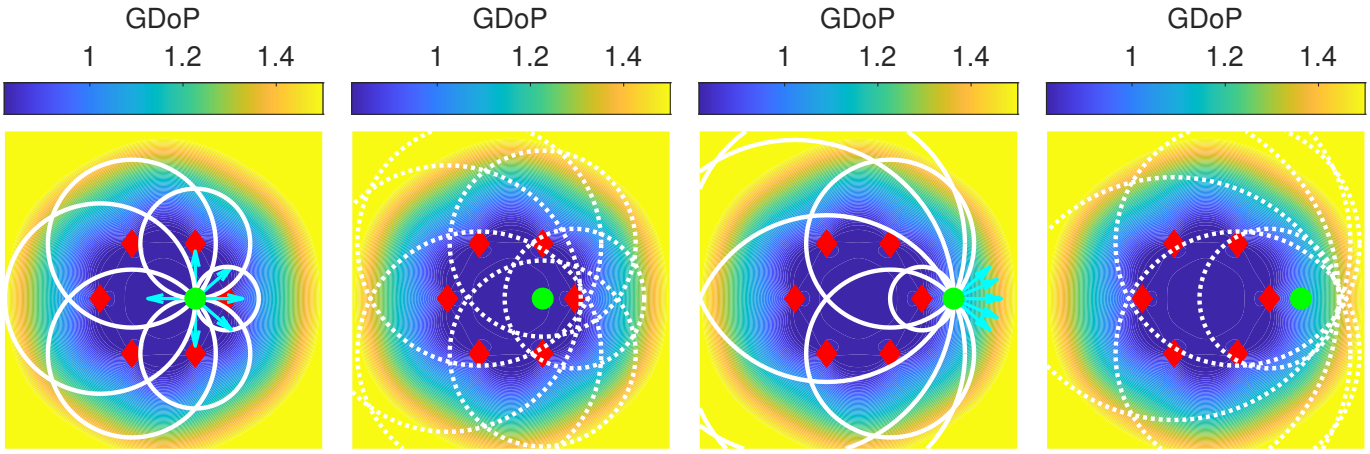
We have shown that a tag, after performing standard TWR with one active anchor, can be localized using either the ToA formulation (Equation 2) or the TDoA formulation (Equation 4). The key difference is that ToA is only accurate if the tag reports its timestamps honestly, while TDoA is accurate regardless 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.

We investigate the accuracy of ToA and TDoA based localization experimentally by placing tags at 13 test locations. The accuracy of deduced tag location is shown in Figure 6 and 7. It's apparent that TDoA-based localization which relies on overlapping hyperbolas has poor dilution of precision at the asymptotes, while ToA-based localization is consistent across all locations. Therefore, TDoA is more suitable for coarse localization of spoofing tags, whereas ToA should be used for more precise localization given that the tag is honest.

B. Dilution of Precision based on Anchor Locations

While ranging imprecision affects the localization accuracy, the placement of the anchor nodes also directly affects the localization accuracy due to dilution of precision (DoP). Effects of high DoP are well-documented in GPS literature [9]. While the effect of DoP is accentuated for the short-range localization in our context, a full treatment of DoP is outside the scope of this paper. We briefly explore the effects of different anchor configurations in Figure 9 and different tag placements in Figure 3.

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



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

Fig. 3: 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.

IV. UnSpoof System Analysis

Section III takes a practitioner's approach and just presents the equations a practitioner should use for a functional UnSpoof system. In this section, we derive these equations and perform clock-drift analysis. The reason accurate localization is possible in UnSpoof is because of robust mitigation of clock-drift effects.

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 Equation 4, 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 Equation 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. Figure 4 shows a CDF comparing the ranging precision of UnSpoof-passive ranging with that for [8] which uses a single sided ranging on a 2D plane around three anchors.

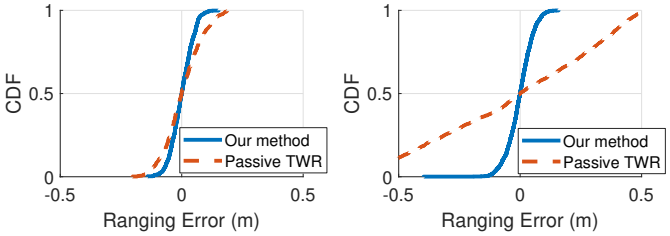


Fig. 4: Comparison between our passive ranging method (Equation 2) and passive TWR [8]. (a) In fast ranging ($D_a \approx 5$ ms), our passive ranging method and passive TWR achieve similar precision. (b) In slow ranging ($D_a \approx 20$ ms), our passive ranging method retains high precision while passive TWR becomes significantly less precise.

V. Implementation

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 $10.39\,sq.m$. This setting allowed us to pre-measure the anchors' locations. Figure 5 shows a photo of our overall setup,

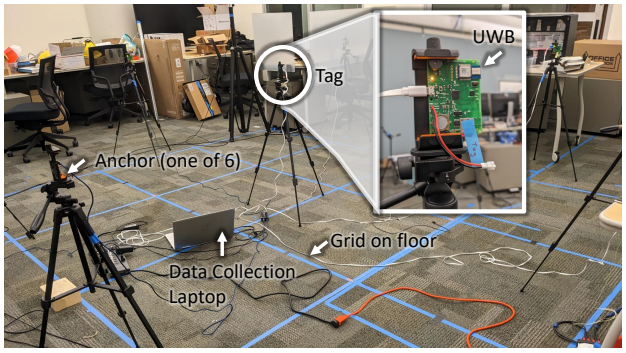


Fig. 5: Our practical implementation of UnSpoof in the lab space. A laptop captures data centrally for processing.

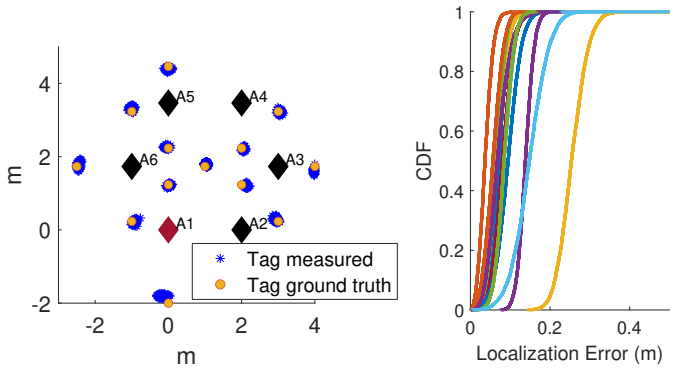


Fig. 6: Localization result using our passive ranging method (Equation 2). (a) Scatterplot of measured tag location at 13 static locations. (b) CDF of localization error across 13 static tag locations.

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. Next, we present the results from our experiments.

VI. Evaluation Results

The tag was placed at several locations in and around the hexagon formed by the anchor devices, running the UnSpoof protocol. Figure 5 illustrates this setup. We now report the evaluation results starting from those for a honest tag.

A. ToA based localization for honest tag

Figure 6 shows the CDFs for the localization result obtained from all the different tag locations. Only ToA 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 ToA (shown in Figure 7). 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.

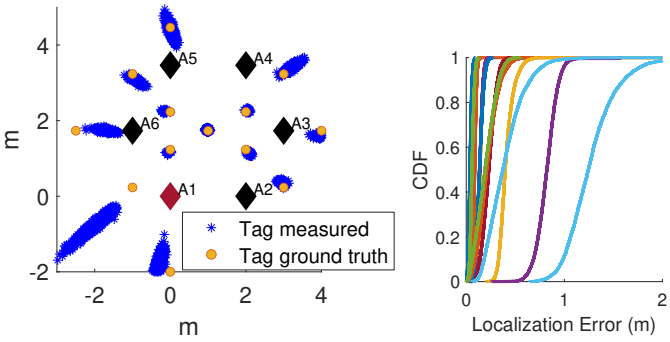


Fig. 7: Localization result using our passive TDoA ranging method (Equation 4) for attacker apprehension. (a) Scatterplot of measured tag location at 13 static locations. (b) CDF of localization error across 13 static tag locations.

C. Spoofing Detection

Given the inaccuracies in ranging, spoofing of distance below a low threshold will go unnoticed. We now investigate the extent of spoofing that will go unnoticed by UnSpoof showing the limitation of our approach.

Figure 8 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 Figure 3c and Figure 3d, where the tag is outside of the convex hull of the anchors. Figure 3c shows the directions of expansion of the range circles in case of distance enlargement 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 Figure 3d), 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 blue streak at the left bottom corner in Figure 7. However, in practice, this is unlikely to happens as anchors are supposed to cover the entire area of interest.

D. 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.

Figure 9 shows that both ToA-based localization and TDoA-based localization suffer poorer localization precision when

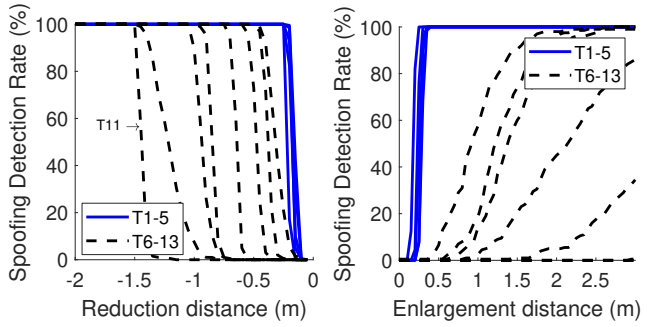


Fig. 8: The spoofing detection rate as a function of spoofing distance for all 13 tag locations. Range reduction is indicated by negative spoofing distance (x-axis), whereas positive spoofing distance indicate range enlargement. The continuous lines and dashed lines are for locations inside and outside the convex-hull created by the anchors respectively.

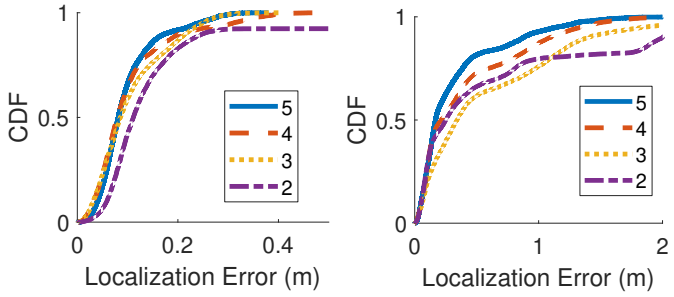


Fig. 9: Localization error CDF under varying number of passive anchors. (a) ToA based localization for honest tag. (b) TDoA based localization for malicious tag.

the number of passive anchors is decreased. This reduction in precision is smaller for ToA than for TDoA.

VII. 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 novel formulation for passive ToA, passive TDoA, and spoofing detection is expected to become a foundational technology for future localization works, and those that use trustworthy localization as a primitive for enabling other applications.

We have made an assumption that all anchor nodes are trustworthy. It would be interesting to see if a fully passive tag system akin to PnPLoc [1] can be similarly developed that detects and ignores if some *anchor* nodes are malicious in a system. UnSpoof increases the processing load at the active anchors, but we leave its quantification to future work. It will also be interesting to create a scalable media access protocol based on UnSpoof allowing multiple tags to collaboratively detect a spoofing tag. How can we maximize the tag's update rate? Obstacles such as walls and furniture generally degrade performance for localization. To what extent will obstacles degrade spoofing detection and tag TDoA localization performance? We leave these questions to future research.

Acknowledgement

This material is based upon work supported by the NSF under Grant No. 2145278.

References

[1] Haige Chen and Ashutosh 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)*, pages 1–8, 2022.

[2] Haige Chen and Ashutosh Dhekne. Pnploc: Uwb based plug & play indoor localization. In *2022 IEEE 12th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, pages 1–8, 2022.

[3] LAN/MAN Standards 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)*, volume 2020. 2020.

[4] Kristof Attila Horvath, Gergely Ill, and Akos Milankovich. Passive extended double-sided two-way ranging algorithm for uwb positioning. *2017 Ninth International Conference on Ubiquitous and Future Networks (ICUFN)*, pages 482–487, 7 2017.

[5] Kristof Attila Horvath, Gergely Ill, and Akos Milankovich. Passive extended double-sided two-way ranging with alternative calculation. *2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband, ICUWB 2017 - Proceedings*, 2018-Janua:1–5, 2018.

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

[7] 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)*, pages 1–174, 2020.

[8] Taavi Laadung, Sander Ulp, Muhammad Mahtab Alam, and Yannick Le Moullec. Active-passive two-way ranging using uwb. *2020 14th International Conference on Signal Processing and Communication Systems (ICSPCS)*, pages 1–5, 12 2020.

[9] Richard B Langley. Dilution of precision. *GPS World*, 10:52–59, 1999.

[10] Patrick Leu, Giovanni Camurati, Alexander Heinrich, Marc Roeschlin, Claudio Anliker, Matthias Hollick, Srdjan Capkun, and Jiska Classen. Ghost peak: Practical distance reduction attacks against HRP UWB ranging. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1343–1359, Boston, MA, August 2022. USENIX Association.

[11] Jorge J. Moré. The levenberg-marquardt algorithm: Implementation and theory. In G. A. Watson, editor, *Numerical Analysis*, pages 105–116, Berlin, Heidelberg, 1978. Springer Berlin Heidelberg.

[12] Dries Neirynck, Eric Luk, and Michael McLaughlin. An alternative double-sided two-way ranging method. *2016 13th Workshop on Positioning, Navigation and Communications (WPNC)*, pages 1–4, 10 2016.

[13] Nils Ole and Nils Ole Tippenhauer. Uwb-based secure ranging and localization.

[14] Baptiste 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.

[15] Mridula Singh, Patrick Leu, AbdelRahman Abdou, and Srdjan Capkun. UWB-ED: Distance enlargement attack detection in Ultra-Wideband. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 73–88, Santa Clara, CA, August 2019. USENIX Association.

[16] Nils Ole Tippenhauer, Heinrich Luecken, Marc Kuhn, and Srdjan 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, 2015. Association for Computing Machinery.

[17] Yiyin Wang, Xiaoli Ma, and Geert Leus. An uwb ranging-based localization strategy with internal attack immunity. In *2010 IEEE International Conference on Ultra-Wideband*, volume 2, pages 1–4, 2010.