Poster: Envisioning a UWB-based Local Human-Machine Interface

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

Ashutosh Dhekne
dhekne@gatech.edu
Georgia Institute of Technology
USA

ABSTRACT

In this work, we present a secure Internet-of-Things framework enabled by UWB, which allows users to wirelessly interact with any public and home appliances in a more secure, seamless and efficient manner. we envision an ecosystem of appliances and mobile devices equipped with UWB transceivers, where the appliances are capable of imposing location-based access control in precise and configurable zones and ensuring security against eavesdropping and hijacking by malicious attackers. We propose a location-based access control algorithm that is robust against range spoofing. Further, we propose the network and application layer protocols that enable one generic user-end application to access the control interface of any appliances and adapt to context.

ACM Reference Format:
Haige Chen and Ashutosh Dhekne. 2024. Poster: Envisioning a UWB-based Local Human-Machine Interface. In *The 30th Annual International Conference On Mobile Computing And Networking (ACM MobiCom '24), November 18–22, 2024, Washington D.C., DC, USA.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3636534.3697464

1 INTRODUCTION

This paper presents a new vision for a secure and seamless user-machine interface centered upon incorporating ultra-wideband (UWB) radios inside household and publicly-shared kiosks and appliances. A few observations prompt us to rethink the ways we interact with appliances today. (1) Appliance touchpads are often the first to break and replacements are costly. This leads to substantial e-waste when consumers have to discard a perfectly functional appliance just because its touchpad cannot be replaced. (2) Touchpads are also an important cause of disease spread particularly when used in public places. Public kiosks in airports and supermarkets and the shared appliances in schools and workplace can become a major source of spreading diseases via fomite transmissions. (3) Eliminating the need of physically interfacing with appliances reduces crowding in public places and maximizes the convenience and efficiency of customers and workers. Therefore, we see significant health, environmental, and social benefits of replacing public appliances with touchless interface enabled by wireless technology.

Home automation based on WiFi, ZigBee, ZWave and BLE exist today, which allow users to control their home appliances from personal mobile devices, and they have proved to enhance the convenience of people's lives. However, we observe two key features necessary for a universal interface which the existing solutions lack: (1) secure location guarantee, and (2) on-the-fly ad-hoc operation. In contrast, UWB brings *precise ranging and localization*, a key capability missing in other wireless technologies, which we believe is the missing piece to fill a crucial gap in local direct connectivity.

Since wireless signals can penetrate through walls, a malicious attacker could appear to be close-by and take control of appliances (such attacks currently affect keyless car entry systems). Therefore, when making appliance control accessible to anyone in proximity, we must ensure that a malicious attacker cannot control the appliances from elsewhere when they do not have physical access to the appliance. We propose a secure localization solution to establish a strict distance and angle relationship between the user and the appliance, which we call the *accessible zone*. Since two-way ranging (TWR) has been shown to be vulnerable under fake-timestamp attacks [3], we propose a verified secure localization method through a combination of angle-of-arrival (AoA), TWR, and time-difference-of-arrival (TDoA) by multiple collaborative trusted appliances. If every appliance included UWB radios, any user with a UWB-enabled mobile phone (or watch) can access the appliance from within the *accessible zone*.

ACM MobiCom '24, November 18–22, 2024, Washington D.C., DC, USA

ACM ISBN 979-8-4007-0489-5/24/11
https://doi.org/10.1145/3636534.3697464

Today many existing commercial home automation solutions require appliances to be connected to the manufacturer's cloud service through an access point, and when a registered user has the correct app on his phone, signed into the manufacturer's cloud service, it is possible to control the connected smart appliance. However, the need for registration and cloud access severely reduces the user's convenience especially when operating publicly shared appliances that is ad-hoc, on-the-fly by nature. To tackle this problem, we propose a novel protocol for communicating the appliance user interface (UI) and the commands over UWB directly that can be customized for different appliances. More specifically, we propose a protocol that reliably transfers the UI in the XML format, and we see an opportunity to re-use the existing Zigbee application layer services over the UWB, such as Zigbee Cluster Library (ZCL), to fulfill the basic functionalities of advertising types of services (e.g. on-off, timed operations), informing appliance's state, and controlling the appliance.

2 PROPOSED SOLUTIONS

At its core, we need to implement two functionalities: (i) allow each appliance to be accessed only from the *accessible zone*, and (ii) enable a customizable user interface protocol for different applications.

2.1 Secure Localization

Single-node localization, where a single appliance can precisely locate the user's phone, requires distance measurements coupled with angle measurements which are possible by combining a two-way ranging (TWR) and phase-difference-of-arrival (PDoA) approach. Decawave's PDoA system [4] provides us with both these functionalities and we expect future appliances will have a similar UWB setup.

However, there is a problem in relying on the two-way ranging measurements since the participating phone could cheat about certain timing information in the packets to drastically alter the measured distance. Usually, since the client benefits from accurate localization, there is little incentive in cheating on the timing information. However, for appliance control, distance spoofing can be quite lucrative since it would allow a malicious entity to access appliances from outside the *accessible zone*. These problems and some solutions to those have been reported recently in other contexts [1–3, 5]. A set of trust-able anchors (or other appliances) are required to overhear the two-way ranging exchange and report the timing of message reception to stop such a location spoofing attack. We have discovered that the availability of AoA and TDoA provides new capabilities that reduce the number of trust-able anchors. Next, we first explore our options for obtaining the user's location and then present our innovations to prevent the user from spoofing.

TWR+AoA: A single anchor can deduce the location of a user using combined distance and angle information as shown in Figure 1. In a relatively small space spanning a few meters, this method results in acceptable localization error close to $10-20\ cm$. However, relying on the two-way ranging protocol for the distance measurement is risky since the tag could potentially alter its reported timestamps, thereby changing its measured distance from the appliance.

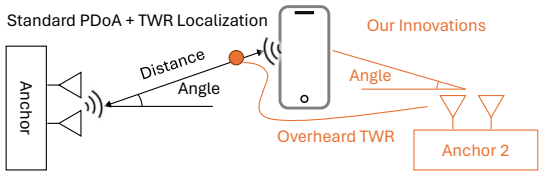


Figure 1: Standard ranging + AoA based single-anchor localization, and our innovation with an additional anchor passively verifying the reported location with TDoA+AoA.

AoA: An alternative arrangement is to use a helper anchor ($A2$) that also performs angle of arrival measurements, without reliance on the ranging measurements. AoA cannot be spoofed by a single antenna mobile phone since it is measured locally and using passive methods. However, since angle measurements are inherently noisy, when combining two angle measurements, the accuracy drops marginally. Further, this method creates a prominent "dead-spot" over the line connecting the two anchors due to a degenerate case.

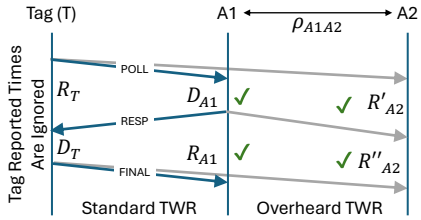
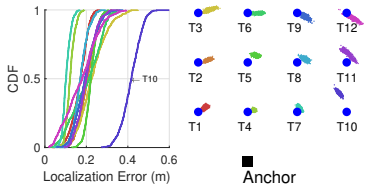


Figure 2: Overhearing an ongoing TWR allows the $A2$ to deduce the TDoA. Adapted from UnSpoof [3].

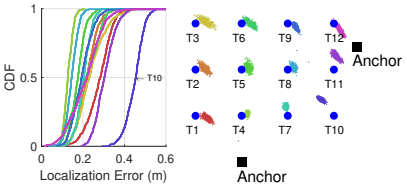
TDoA: A third approach, inspired by the recent treatment in UnSpoof [3], is for the second anchor to passively overhear the TWR being performed between the first anchor and the tag. Ignoring the spoof-able timings reported by the tag, it is possible to derive the TDoA hyperbolic locus. We have adapted Figure 2 from UnSpoof [3] here as Figure 2 for completeness. The TDoA is then given by:

$$T_{A1A2} = \rho_{A1A2} - \frac{R_{A1}R'_{A2} - R''_{A2}D_{A1}}{R_{A1} + D_{A1}} \quad (1)$$

Combining TDoA and AoA: The arrangement combining TDoA with the AoA from both anchors is shown in Figure 1. We experimentally verify this method by setting up two PDoA anchors (Decawave DW1002) and moving one tag device (Decawave DW1000) to 12 locations shown in Fig. 3. It shows that by combining TDoA and AoA which cannot be spoofed by the fake-timestamp attack, the localization precision is slightly worse than but comparable to the TWR+AoA solution which could be spoofed.



(a) TWR+AoA from Single Anchor



(b) AoA from Anchor 1, AoA+TDoA from Anchor 2

Figure 3: Localization scatterplot and error CDF for 12 static tag locations.

We have seen above that using two PDoA anchors, potentially embedded into two different appliances, the user's location can be verified without relying on any information that the user can spoof. However, we obtain a higher precision location using AoA+TWR method and therefore, we use a two-phased approach as presented in Figure 4. We first calculate the reported location using the TWR+AoA method. Then we verify whether this location is within a small distance-bound from the location obtained by the passive AoA+TDoA+AoA method. If successfully verified, we use the original TWR+AoA location with higher precision to tell whether the user is inside the *accessible* region or not. If the two methods do not agree on the tag's location, a spoofing tag is detected and an alarm is raised. Next, we discuss how the appliance user interface and the control signals can be communicated over UWB.

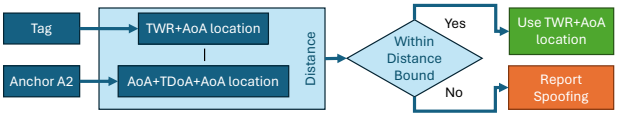


Figure 4: Every tag-reported location is verified using information from another trustworthy anchor.

2.2 Transferring Appliance UI via UWB

After the user's location has been verified relative to the appliance, the appliance UI should be transferred to the smartphone and the appliance should await user input from the smartphone. For graphical layout, Android allows rendering of an XML-based layout providing all the various UI elements needed to show the variety of buttons, knobs, and sliders, etc. on the phone's screen. Therefore, an XML file can be transferred over UWB and rendered on the mobile device. The second aspect of UI is the continuous interaction between the appliance and the mobile device–some required

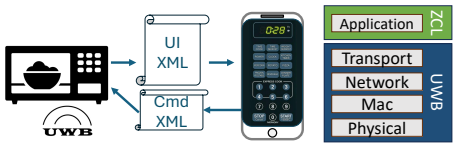


Figure 5: The UI Rendering is described by a standard XML file. The Zigbee application layer services can be re-used over UWB for appliance control.

services include (1) advertising the type of services that the appliance support, (2) informing the status of the appliance, (3) controlling the appliance. Interestingly, these functionalities already exist in the Zigbee application layer services, such as the ZCL, that can be re-used over UWB (see Figure 5). A key innovation in this space is that a single generic app can render the UI of any appliance from any brand since the appliances use a standard format to report the expected UI. We keep images and other large data items to a minimum in this UI data transfer to allow fast UI transfer to the smartphone. Figure 5 shows this data flow. When the user presses a button on the phone, a small command worth a few bytes is sent to the appliance over UWB. Sending entire microwave UI takes only a few hundred milliseconds in our tests.

3 CONCLUSIONS

We present a UWB-based solution for securely interfacing with home and publicly-shared appliances. Leveraging UWB's precise localization capabilities, we propose an anti-spoofing localization scheme that allow appliances to have finely-defined *accessible zone* to prevent illegal access from attackers, and a protocol enabling UI over direct UWB links.

REFERENCES

[1] Srdjan Capkun, Kasper Rasmussen, Mario Cagalj, and Mani Srivastava. 2008. Secure Location Verification with Hidden and Mobile Base Stations. *IEEE Transactions on Mobile Computing* 7, 4 (2008), 470–483. https://doi.org/10.1109/TMC.2007.70782

[2] Haige Chen and Ashutosh Dhekne. 2023. Spoofing Evident and Spoofing Deterrent Localization using Ultra-wideband (UWB) Active-Passive Ranging. *IEEE Journal of Indoor and Seamless Positioning and Navigation* (2023), 1–13. https://doi.org/10.1109/JISPIN.2023.3343336

[3] Haige Chen and Ashutosh Dhekne. 2023. UnSpoof: Distance Spoofing-Evident Localization using UWB. In *2023 IEEE 13th International Conference on Indoor Positioning and Indoor Navigation (IPIN)*. 1–6. https://doi.org/10.1109/IPIN57070.2023.10332533

[4] Igor Dotlic, Andrew Connell, Hang Ma, Jeff Clancy, and Michael McLaughlin. 2017. Angle of arrival estimation using decawave DW1000 integrated circuits. In *2017 14th Workshop on Positioning, Navigation and Communications (WPNC)*. 1–6. https://doi.org/10.1109/WPNC.2017.8250079

[5] Patrick Leu, Giovanni Camurati, Alexander Heinrich, Marc Roeschlin, Claudio Anliker, Matthias Hollick, Srdjan Capkun, and Jiska Classen. 2022. Ghost Peak: Practical Distance Reduction Attacks Against HRP UWB Ranging. In *31st USENIX Security Symposium (USENIX Security 22)*. USENIX Association, Boston, MA, 1343–1359. https://www.usenix.org/conference/usenixsecurity22/presentation/leu