IntruSense: An Enhanced Physical Security System using UWB

Shrenik Changede
Ashutosh Dhekne
Georgia Institute of Technology
USA

ABSTRACT

A wireless signal travels through various paths and reaches a receiver multiple times. These paths remain fairly stable in an undisturbed environment if nothing is moving in the space. However, if humans are present in such a space, reflections from their bodies will constantly alter the multi-path behavior of the wireless signals and cause disturbances in the received wireless power-delay profile. This work explores various ways in which such signal disturbances can be used to perform intrusion detection providing an enhanced physical security system. Since wireless signals can pass through walls, they can monitor a larger multi-room area without requiring additional hardware. We further explore if it is possible to allow a friendly entity, such as a pet or a guard, to freely move in the monitored space without triggering an alarm, and yet remain vigilant about intrusions into the home. This work explores using wireless disturbances in 4 modes: (1) line-of-sight obstruction, (2) detecting proximal movements, (3) separating friendly movements, (4) using minimal infrastructure. We demonstrate intrusion detection capabilities using ultra-wideband (UWB) wireless radios. Our preliminary results show promise, and we feel confident that this work will open up a new direction for physical security spanning use cases such as home security, security of high-value public spaces (such as museums), and industrial security.

CCS CONCEPTS

• **Computer systems organization** → **Sensors and actuators**; • **Human-centered computing** → *Ubiquitous and mobile computing systems and tools.*

KEYWORDS

UWB, Physical Security, Wireless Sensing, Indoor Security, Fencing Systems, Channel Impulse Response, Home monitoring

1 INTRODUCTION

This paper explores the use of disturbances created in wireless signals due to human movements as a mechanism to detect intrusion of a physical space. Wireless signals pass through walls [8] and cover a much larger space [11] than currently available infrared-based motion sensors. Therefore, use of wireless signals for intrusion detection is expected to require fewer sensors and avoid blind spots. Furthermore, it can also enable friendly entities, such as pets or guards, to freely move in the protected space by ignoring movements in the specific area where the pets or guards are currently present—a feature that no existing system can provide.

Physical security is a multi-billion dollar industry and is expected to increase substantially in the near future [13]. While the industry has seen much growth and has transformed to an IoT based service industry, the techniques it has relied upon to detect intrusion have been limited. Primarily, intrusion is detected by magnetic door and window sensors or by IR-based motion sensors installed inside rooms. Cameras are frequently used to validate intrusion after an alarm is triggered by the magnetic or IR sensors. A major issue faced by the security industry is that since cameras and IR sensors can only "see" one room at a time, numerous devices are required to secure a typical indoor space. Furthermore, movements of house pets frequently trigger alarms in home settings, and high-value places such as museums need active guards on duty which would also cause the IR based or camera based security system to constantly raise an alarm. We will address such friendly entities (pets, guards, etc.) that are expected in an environment, as *friendlies.* In this work, we ask the question: *Can wireless signals help in creating a more robust intrusion system and allow friendlies to freely move around in the monitored space?*

In trying to answer this question in the affirmative, we observe that various levels of expectations exist for intrusion detection systems. A desire to monitor *ingress and egress points* would lead to the need for a line-of-sight blockage detector similar to a laser. Alternatively, one may desire a different form of intrusion detection system where an indoor *space* is protected such that an alarm is raised if anything moves in that space. Yet another desire might be to *ignore movements of a known entity* like a pet or an elderly person in the house while still monitoring for other intrusions; a desire that is not currently satisfied by any available system. Today's security systems have a "home" mode which ignores internal movements completely and instead only monitors the ingress/egress points.

Wireless signals provide an obvious benefit over lasers or camera based systems; they can penetrate through walls [3] and therefore fewer individual units can suffice for monitoring an entire house or a large part of a museum. However, using wireless signals for this purpose is not straightforward. Wireless signals cannot be pinpointed like lasers and therefore are less precise for scanning an area. Similarly, wireless signal strength is unreliable in most settings. *What hope do we then have to enable a wireless intrusion detection system?* In exploring the various available wireless technologies to base our study on, the recent advances in ultra-wideband (UWB) radios come to forefront. UWB radios use a large bandwidth signal and their primary use is in wireless localization. Due to the large bandwidth, UWB receivers are able to assess the direct line of sight better than other wireless technologies such as Bluetooth and

HotMobile '22, March 9–10, 2022, Tempe, AZ, USA

ACM ISBN 978-1-4503-9218-1/22/03…$15.00
https://doi.org/10.1145/3508396.3512884

Wi-Fi. Furthermore, UWB receivers can also separate out close-by reflected paths in the time domain and obtain a detailed channel impulse response (CIR). Since the UWB pulse is wider than 1 *ns* , the effect of an obstruction is felt beyond one tap causing all reflections to be accounted for, so long as the reflecting surface is larger than the wavelength of the UWB signal (about 7.5 *cm*). These capabilities are promising and could form the bed-rock of IntruSense.

This work takes an exploratory approach towards the problem of intrusion sensing using wireless signals. To that end, we perform rather simplistic experiments within one household to validate the base ideas that will enable a more complete system. For example, while we collect real data with human movements, we have not tested IntruSense in a variety of environmental settings, we perform the analysis of CIR as a post-processing step, and do not have an end to end real-time ringing of alarms. The transmitted wireless signals are real (not simulated), though, and their disturbances due to human movements are also recorded on a physical device. We intend to release the software code for the UWB hardware and the CIR analysis code in the public domain, facilitating other researchers to easily advance this field.

2 BACKGROUND

The distance between two wireless devices can be inferred from the duration of time it takes wireless signals to travel from one device to the other, and multiplying it with the speed of light ($3 \times 10^8 m/s$), which requires precise clocks. Advancements in ultra-wideband (UWB) radios have made multi-GHz sampling rates possible, and have pulses spanning just a few nanoseconds. Together, this **enables nanosecond level precision of detecting signal arrival times**. Commercially available IoT devices now exist that have UWB capabilities [9], and more recently, the first few smartphones with UWB have been announced [10; 20]. Thus, UWB is likely to become commonplace in the near future, on mobile and on infrastructure devices, just like Wi-Fi.

Channel Impulse Response: Due to the large bandwidth, it becomes possible to discern various echoes or copies of a wireless signal arriving over time, just nanoseconds apart. A time-domain plot of successive echoes describes the complexities of the wireless channel. These echoes can be represented as a sequence of *impulses*, called the channel impulse response (CIR); a sequence of pulses are obtained when echoes exist. In an indoor environment with many reflecting surfaces, multiple close-arriving echoes would exist due to multi-path, while in an empty outdoor environment, there would be hardly any echoes (see Fig. 1).

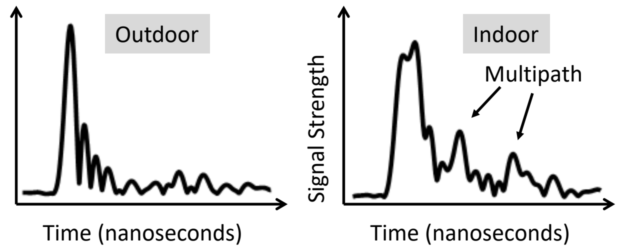
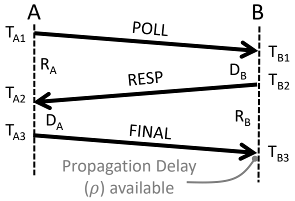


Figure 1: The CIR shows multipath reflections in a room. Reflections are less outdoors.



$$R_A = T_{A2} - T_{A1}, \quad R_B = T_{B3} - T_{B2}$$

$$D_B = T_{B2} - T_{B1}, \quad D_A = T_{A3} - T_{A2}$$

$$\boldsymbol{\rho = \frac{(R_A - D_B) + (R_B - D_A)}{4}}$$

$$\boldsymbol{\rho = \frac{(R_A R_B - D_A D_B)}{R_A + R_B + D_A + D_B}}$$

Figure 2: The standard IEEE 802.15.4 ranging protocol [16] with the alternative formulation from [22].

Two-way Ranging Protocol (TWR): A ping-pong message exchange with both devices sending one wireless packet each is required to eliminate device-clock offsets. However, at the timescale of interest (nanoseconds), eliminating the clock-offset will not be sufficient, since clocks also *drift*. Compensating for drifts requires a third wireless packet to be sent. The IEEE 802.15.4 [16; 18] has standardized a symmetric two way ranging (TWR) scheme shown in Fig. 2 which minimizes effect of clock offsets and clock-drifts.

3 SYSTEM DESIGN

The core idea of IntruSense is that carefully analyzing disturbances of wireless signals can help detect intrusion into a space. The specific needs in a space may vary, though, and we will take into account these differences of needs when presenting our system design. In fact, we will present the various capabilities as different "models" of intrusion sensors, almost as if these are product offerings.

3.1 Model 1: Line-of-sight Obstruction

Fig. 3 depicts the intrusion detection mechanism for Model 1. Here, we expect a static UWB device pair to be placed across ingress or egress points, such as across a doorway. The two devices would constantly measure the distance between them using the standard IEEE 802.15.4z ranging protocol. Of course, since the two devices are static, they will measure the same distance continuously. We expect only a small fluctuation in these distance measurements due to hardware imperfections. Our stability analysis (see the "No LOS obstruction" line in Fig. 3(b)) matches several published results [18]; within 10 *cm* at the 95^{th}*percentile*.

When a person crosses the direct path between the two UWB devices, the first arriving path gets attenuated, and might even get blocked completely. For the UWB devices, a later arriving path might seem as the first arriving path which corresponds to a different, longer distance measurement. Thus, an increase in the measured distance at the UWB devices would indicate intrusion (see the "LOS obstruction" line in Fig. 3(b)). For this mechanism to work, we must ensure that: (1) an intruder cannot "crawl under" the direct path, and (2) an intruder will be detected even if they

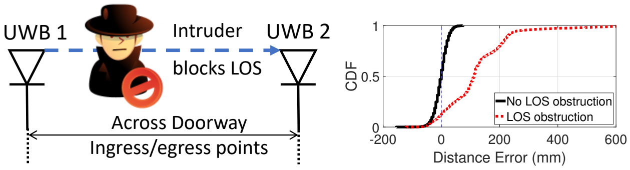


Figure 3: (a) Model 1 Architecture, (b) Distance measurements with and without LOS obstruction. (Each CDF contains hundreds of measurements with discrete mm-level distances, causing a jagged line.)

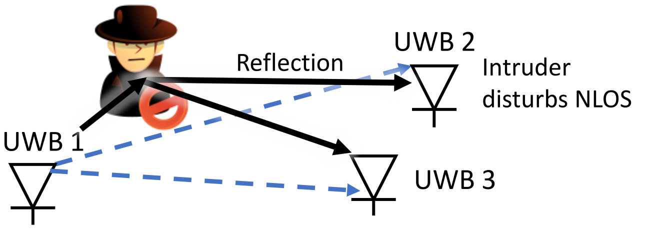


Figure 4: Model 2 detects intrusion even though the LOS is not obstructed by the intruder.

run fast through the entrance. Ensuring (1) is easier in wireless signals than in single beam lasers. Wireless signals spread out in all directions, and the first path detection occurs over a pulse 3-4 nanoseconds wide. This means that, even if there are disturbances within a few feet, it influences the first path detection and therefore the distance estimation. Ensuring (2) requires a sufficiently high rate of distance measurements. Considering the maximum speed of running through the barrier as $5\,m/s(11mph)$, and the first-path influence zone as 1 meter, a measurement once every 200ms will suffice to detect an anomalous distance measurement. In our preliminary tests, we have obtained about $10\,Hz$ update rate, with further improvements possible through protocol optimizations.

Limitations of Model 1: Practically deploying Model 1 would require *every* ingress and egress point to be protected by a UWB device pair. Furthermore, the internal space would remain vulnerable to unconventional ingress/egress point being exploited (such as through an HVAC vent, or boring through the floor). Model 2 which detects disturbances beyond the first path can overcome this limitation.

3.2 Model 2: Non-line-of-sight Disturbance

Often times, a space needs guarding, but ingress/egress points are not a suitable venue for intrusion detection. There could be several reasons for this: in a museum a particular artifact in the center of the room might need its own added layer of security (no obvious ingress/egress cross points), or the protected artifact might be outdoors, or the space could be vulnerable to brute-force egress point creation (breaking the skylight, or digging through the floor, etc.). Model 2 provides a potential solution by observing disturbances to the wireless signals by non-line-of-sight reflections.

The core intuition is to not use changes in the distance measurements, which are influenced only by line-of-sight (LOS) obstructions, but instead to analyze non-line-of-sight (NLOS) disturbances of wireless signals (see Fig. 4). In general, a UWB device that only provides distance measurements will ignore such NLOS disturbances. However it is possible to extract the UWB CIR which provides a means to analyze various reflections arriving at the receiver. In an unoccupied environment, these reflections and the first arriving path remains fairly stable over time, establishing a pattern of echoes. However, if an intruder enters this space, the reflections from the intruder will cause new patterns of echoes.

Model 2 provides additional advantages over Model 1. Since the changes to the CIR occur for every transmitted wireless packet, a UWB pair need not calculate distances at all, and we can eliminate the use of TWR. This observation makes it possible to add an arbitrary number of receiver devices in the environment while still using a single UWB transmitter; each transmitted packet will be received by all receivers and its CIR analyzed. Thus, Model 2 is a fully scalable solution for intrusion detection. Furthermore, since the transmitter need not wait for a response, update rate can be extremely high, only bottlenecked by the rate at which CIR can be processed by the receiver.

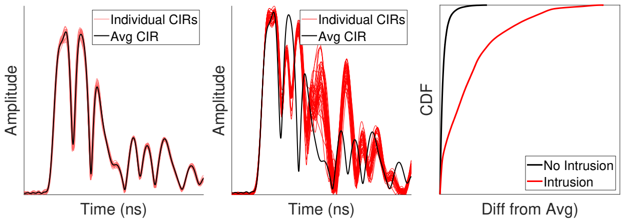


Figure 5: A CIR records all echoes of transmitted wireless signals. (a) Echoes remain stable for an unoccupied room, whereas (b) echoes are recorded when a person moves about in the vicinity. (c) A CIR that deviates significantly from the average gets flagged as intrusion.

To simplify comparison between CIRs, we allow capturing of CIRs during a short initial period which is guaranteed to be intrusion-free. An average CIR is computed for this duration. Then, every incoming packet's CIR is compared to that of the average obtained during the guaranteed intrusion free period. We use the Kolmogorov–Smirnov [21; 23] test to determine if the new incoming CIR's difference from the average belongs to the same distribution as the data collected when the room was unoccupied. If two consecutive packets are deemed to be different, an alarm is raised. Fig. 5 shows the difference between 100 CIRs in an unoccupied room, its computed average, and 100 CIRs when a person is moving inside the room, and the CDFs produced by the two.

It is also possible to layout a perimeter of interest for intrusion monitoring. The CIR provides direct means of defining a perimeter. Each tap on the CIR corresponds to a particular distance, increasing in the granularity of $1\,ns \approx 1\,foot$. By ignoring changes in the CIR beyond a certain tap, a specific boundary can be enabled, but we leave it to future work.

Limitations of Model 2: Model 2 still lacks the ability to ignore disturbances created by friendly entities. It is only a marginal improvement over IR based motion monitoring devices since it can cover a larger space. We explore ignoring movements of friendlies in Model 3.

3.3 Model 3: Protecting Occupied Spaces

While intrusion detection seems to be most important for unoccupied spaces, the need for intrusion detection also extends to cases where a pet or an elderly person is already occupying the monitored space. This is frequently termed as the "Home" mode in security systems. Typically, only ingress/egress points are monitored in this mode and motion sensors are ignored. However, theft and trespassing of occupied premises is a significant risk to property and life. When intrusion detection systems rely on video monitoring, friendlies have to be registered with the monitoring agency. Yet, this approach is privacy intrusive, generates a lot of data and needs sufficient light to work well. On the other hand, our UWB based sensors are privacy preserving (no videography), produce a minuscule amount of data, and work even in complete darkness. Furthermore, UWB range goes across rooms and therefore IntruSense

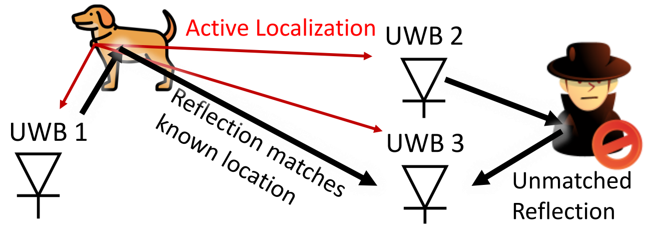


Figure 6: Obtained reflections from a friendly entity match well with the expected pattern deduced from their location. Mismatch with intruder's reflections raises alarm.

requires minimal hardware. We now explore ways in which wireless intrusion detection can help create a safer environment for the occupants.

Wireless signals reflecting from a person's body create disturbances in the observed CIR. Since the reflected path is longer than the direct path, the CIR disturbances are observable in the time domain as if starting at some time after the initial direct path signal arrives (a few nanoseconds of delay). This time delay, which is just the extra path length of the reflected path, provides a clue about *where* the source of the disturbance is located. With a single observation, the locus of possible locations is an ellipse. When combined with observations from multiple UWB receivers, it becomes possible to localize the disturbance. This forms the key intuition in compensating for movements of a friendly entity.

In Model 3, we require the friendly entity to wear a UWB device—a UWB smartwatch for an elderly person or a UWB collar for a pet—which performs localization with installed anchors in the indoor space. As a result, the location of the friendly is already known to the system (see Fig. 6[1]). Using this location, we can estimate *the reflection path delay* for signal reflections from the person's body with respect to the anchors' locations. We expect that the observed CIR will be identical to the CIR obtained in the unoccupied room up to the extra delay of the reflected path. After this point, the CIR might have more disturbances due to the influence on the second and higher order reflections. The system can now ignore CIR disturbances consistent with this knowledge of the friendly's location and yet continue to monitor the space for intrusions. Fig. 7 shows an example CIR obtained when a person is standing such that the extra path length is about 5ft over the direct path. The observed CIR matches the unoccupied CIR up to the indicated vertical line, after which, the occupied CIR diverges. When the CIR diverges inconsistent with the friendly's location an alarm is raised.

Limitations of Model 3: Since the UWB anchors are installed at a substantial distance from each other, the reflected path lengths frequently come close to the direct path lengths. Since CIR taps after the friendly's reflections are somewhat unusable, the effective secure area under monitoring could get reduced significantly. Further, the system requires installation of multiple UWB anchors in the user's environment which can be cumbersome. With an eye towards overcoming these limitations, we introduce Model 4, which proposes creating a UWB radar.

[1] Pet icon from https://www.flaticon.com/ (Free with attribution.), no animals were used in this study.

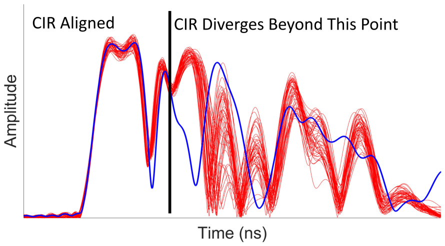


Figure 7: Initial part of CIR is similar to the unoccupied room's CIR. Starting from the path length delay of the reflection from the friendly, the CIR diverges.

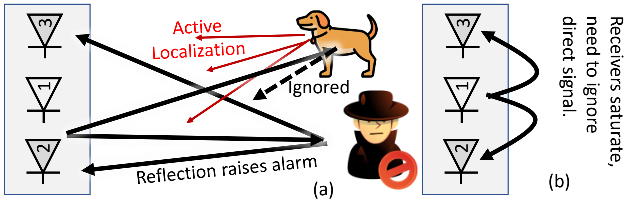


Figure 8: (a) A single box containing multiple UWB devices could detect disturbances to transmitted signals caused by reflections in the vicinity. (b) The main challenge arises from saturated receivers due to the transmitter proximity.

3.4 Model 4: Monitoring from a single spot

A physical setup that requires multiple UWB devices to be installed in an indoor space can become cumbersome. An ideal system would be a self-contained single box that can house all necessary hardware for monitoring unauthorized movements in the environment. Of course, a friendly entity would still carry their own UWB radio to signal their location, which will be ignored by the system. Fig. 8 shows the envisioned setup with collocated UWB devices.

A major hurdle in creating a UWB setup as shown in Fig. 8 is that the transmitter and the receiver are very close to each other. Therefore, the signal strength of the nearby transmitter saturates the receiver, effectively blinding it to any weaker reflections received from the environment. We postulate that a two-antenna phase synchronized transmitter could potentially create a "null-zone" around the receivers so that the signal strength of the direct path signal is substantially reduced [3], without any precoding of the transmitted signal. While **we leave implementing Model 4 to future work**, we would like to highlight its benefits over Model 3. Since the transmitter and receiver are close to each other, the presence of friendlies cause smaller blind spots for the system. As the whole system is contained within a single box, it is harder to forcefully disable, such as by plugging the device out.

3.5 Avoiding Impersonation of Friendlies

Ignoring movements of friendlies might seem like a fundamental vulnerability. To prevent an intruder from creating an **impersonating UWB device**, we plan to secure UWB messages against such attacks using seeded CSPRN generators, so that the receivers know which numbers will be generated by the friendly UWB device. This will raise an alarm if a transmitter device is impersonated.

4 IMPLEMENTATION

The IntruSense system is implemented using custom built UWB devices originally developed for the 6FitAPart project [8] as anchors and as devices carried by the friendlies. We use Decawave DW1000 UWB chips [9], which are controlled by the Cortex M0 microcontroller. Every device is equipped with a buzzer; it is sounded on intrusion. Data collected from these devices, including distance estimates and the CIRs, was streamed to and stored on an Intel Core i5 computer running Microsoft Windows. The data was post-processed in Matlab. The experiments were performed in a single indoor space, and the authors performed the user-actions for evaluation.

5 EVALUATION

5.1 Model 1: LOS Obstruction

Two UWB devices continuously measuring distance between them were placed about 1.8m apart. Fig. 9 shows the obtained distance for a 3 minute duration. A person repeatedly cut through the LOS between the two devices during the middle one minute duration. The LOS obstruction is clearly observable as the larger reported distance measurements. A simple threshold based classifier is sufficient to identify intrusion.

5.2 Model 2: NLOS Disturbances

Model 2 was evaluated using a three device setup where one of the UWB devices was a transmitter and the other two were receivers. The devices were allowed to run in an unoccupied room for several minutes and an average CIR was calculated. One of the researchers then entered the room and moved around for several minutes. For every new CIR generated, IntruSense algorithm output whether or not an intrusion has occurred. Fig. 10 shows the CDF of deviation from the average observed with and without intrusion. The K-S test is able to correctly classify most intrusion events.

5.3 Model 3: Protecting Occupied Spaces

Three static anchor devices were placed in the room, while a fourth device, called the friendly device was also kept static. It performed two-way-ranging (TWR) with the 3 anchors to constantly allow the anchors to compute the location of the friendly device. The CIR remained stable similar to Model 2. Next, a person carried the friendly UWB device and only fidgeted with the device in hand (small movements). We observe that the first few taps of the CIR coincide with the unoccupied room CIR while the later taps show variations, as expected. Finally, another person (intruder) moved in this room without wearing a UWB device and we observed substantially higher variations (see Fig. 11).

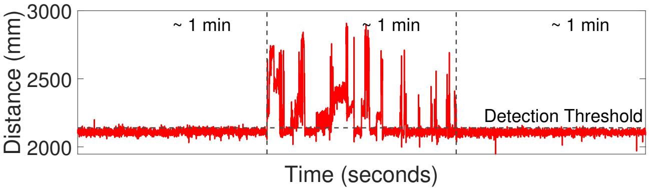
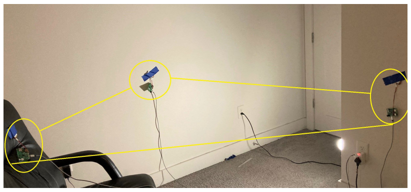


Figure 9: Distance measurements affected by a person moving through the line-of-sight; 95% detection threshold.



Classification	No of packets
Correct class	93
Incorrect class	7

Figure 10: (a) Our test setup with 3 UWB devices and the indoor space to be monitored (b) The KS classification results for a few example windowed CIR difference values for Model 2.

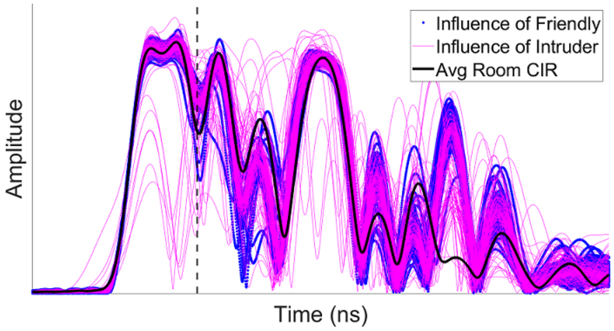


Figure 11: Influence of a static friendly and a moving intruder on the CIR

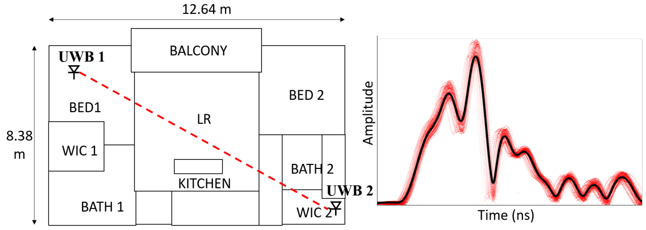


Figure 12: CIR for an entire house with devices kept at boundary points for determining coverage range.

5.4 IntruSense Range in Real-world Settings

UWB uses low-power transmissions [16] and therefore is thought to be short-range. However, the reduced data rate (110 *kbps*) coupled with a large bandwidth allows UWB transmissions to span large indoor spaces. Several existing research works use UWB devices to span large indoor spaces [11; 15]. To ascertain its utility in our use-cases, we installed the UWB devices in a household, and performed ranging experiments to determine coverage. Without obstructions, line of sight (LoS) path between the two devices was measured up to 18.87 *m*. Our indoor space did not allow for longer distances. With obstructions in the LoS, this range was reliably measurable up to 15 *meters*. Fig. 12 shows the layout of the student apartment where the experiment was performed along with the CIR obtained when the two devices were kept at two extreme ends of the house. We thus conclude that with current specifications and while remaining FCC compliant, the UWB devices can easily span an average 2-bedroom apartment (1200 square feet). Theoretically, as mentioned in official product documentation of DW1000[1], and from Decawave (now Qorvo) discussion forums[2], device ranges can be extended to 300 *meters* [1] by either increasing transmission power of the transmitter or increasing sensitivity of the receiver device. Hence, the Decawave devices can be easily modified to span entire households.

6 RELATED WORK

Use of IoT in physical security has grown significantly over the past few years [24; 25]. However, these studies do not use wireless sensing modality for intrusion detection. Perhaps closest to our work is the work of Withington *et al.* [26] where the authors use short-range UWB radar to create a robust perimeter security systems for exterior installations. They bolster our claim that wireless sensing provides an excellent means for through-wall movement detection. However, in contrast to IntruSense, they do not provide the ability to ignore movements of friendlies, or to create ingress/egress barriers. Yang Junjie *et al.* [19] have shown how ZigBee devices can become part of long distance communication of security events. Several commercial systems also use Zigbee in similar fashion [4; 17]. IntruSense uses UWB as a sensor and not just as a communication protocol. Boselli *et al.* [6] have explored perimeter fencing by proposing attaching a module, called the Airport Secure Perimeter Control System to small unmanned aircrafts to prevent runway incursion of the same with commercial airplanes. To some extent, this idea overlaps with our idea of using a UWB device. However, it differs in that we require putting a device only on friendlies, while [6] requires such a module on intruders as well, weakening the protection from rouge actors. Brugarolas *et al.* [7] have researched in depth about wireless pet tracking and training systems, which gives a wide view of short range communication and action based on breach of a pre-designed perimeter. In contrast to intrusion detection, the main goal in [7] is to train pets, though it shows the practicality of a Bluetooth enabled pet collar, which would be similar to what we will require in IntruSense. Ghatak *et al.* [14] have explored the use of IR and microwave in combination with a wireless camera for development of a wall mounted intrusion detection system and transfer the information to a central station for processing using a wireless mesh network. Yet, no work has been done on the problem of ignoring the movements of a friendly. Wireless sensing has been explored in recent years [3; 12; 27] and communication technologies like Bluetooth, Wi-Fi, ZigBee have been used for the same. However none of these use wireless sensing for intrusion detection. UWB has received significant attention in recent years [8], however, their use for intrusion detection is under studied. In summary, the use of UWB-based wireless sensing for intrusion detection, and in particular allowing friendly entities to occupy the space, is an under-explored area. We hope IntruSense will accelerate interest in this area.

7 CONCLUDING REMARKS

Limitations of IntruSense: Despite being sensitive to most intrusive actions, IntruSense is susceptible to few attacks, which we address next. Metallic objects effectively block radio-frequency signals and UWB is no exception. In case an indoor space has a continuous line of metallic furniture, the area behind this furniture (away from the IntruSense sensor) is hidden from IntruSense's view. An intruder traversing this shadow can intrude into a space without detection. An effective counter strategy is to install IntruSense devices on opposite walls which minimizes such hidden spots. An intruder cannot simply use a metallic shield, of course, since that will cause deviation of the reflected signals from the known room signature. Another limitation stems from non-reflecting intruders. Robotic models that do not have metallic parts and are small in size could move undetected under IntruSense. Supplementary sensors will be required in spaces where such attacks are a threat. Unauthorized devices can hack into the system and assume identity of one or more friendly devices and malfunction to allow intrusion. This can be prevented by using light weight ciphers[5] to cryptographically encrypt IDs of the devices, which will help prevent hacking. Another type of attack is to cause physical damage to the devices to prevent them from working without human intervention. This can seem as an accident and might go unnoticed. We can deploy multiple devices to avoid this. Also, timely message exchanges can guarantee the safety and working of each device. We can assume devices to be compromised or tampered with if they fail to participate in these timely message exchanges.

A Tx-Rx pair forms an ellipse that has the same reflection time. This raises ambiguity in localization and intrusion sensing. We can resolve this by increasing device pairs. Two device pairs will result in two ellipses, which will reduce ambiguity to two points. If three pairs are used, there will be no ambiguity. In IntruSense, Model 1 and Model 2 are unaffected by this, and for Model 3, we can use 3 devices to solve this problem. Model 4 has a bilateral symmetry in front and back of the single-box device.

Closing Thoughts: Despite the many advancements in security systems over the years, certain features such as allowing friendly entities to freely use a protected space are elusive to traditional methods. UWB provides a viable alternative with its ability to scan an entire household with minimal hardware, while ignoring disturbances to wireless signals caused by friendlies such as pets, the elderly, and security guards. Compared to cameras which are expensive to install, are privacy invasive, produce a large amount of data, and are needed in every room, IntruSense's wireless sensing provides a relatively inexpensive and privacy preserving option. We expect IntruSense to inspire future researchers to explore wireless sensing as a mechanism for physical security.

REFERENCES

[1] Decawave dw1000 product brief, 2013.

[2] Decawave discussion forum, 2017.

[3] Fadel Adib and Dina Katabi. See through walls with wifi! In *Proceedings of the ACM SIGCOMM 2013 conference on SIGCOMM*, pages 75–86, 2013.

[4] Arbab Waheed Ahmad and et al. Implementation of zigbee-gsm based home security monitoring. In *MWSCAS 2011.*

[5] Aydin Aysu, Ege Gulcan, and Patrick Schaumont. Simon says: Break area records of block ciphers on fpgas. *IEEE Embedded Systems Letters*, 6(2):37–40, 2014.

[6] Chris Boselli and et al. Geo-fencing to secure airport perimeter against suas. *International Journal of Intelligent Unmanned Systems*, 2017.

[7] Rita Brugarolas and et al. Wearable wireless biophotonic and biopotential sensors for canine health monitoring. In *SENSORS, 2014 IEEE.*

[8] Yifeng Cao, Ashutosh Dhekne, and Mostafa Ammar. 6fit-a-part: A protocol for physical distancing on a custom wearable device. In *2020 IEEE 28th International Conference on Network Protocols (ICNP).*

[9] DecaWave. DW1000 User Manual. https://decawave.com/content/dw1000-user-manual. https://decawave.com/content/dw1000-user-manual".

[10] Android Developer. Google adds ultra-wideband (uwb) api to android with focus on smart homes. https://bit.ly/3qpFaeI, 2020.

[11] Ashutosh Dhekne, Ayon Chakraborty, Karthikeyan Sundaresan, and Sampath Rangarajan. Trackio: tracking first responders inside-out. In {*NSDI*} *19*, pages 751–764, 2019.

[12] Lijie Fan, Tianhong Li, Yuan Yuan, and Dina Katabi. In-home daily-life captioning using radio signals. In *Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020.*

[13] Financialnewsmedia.com. Home security systems market could exceed $78 billion by 2025, 2020. https://www.prnewswire.com/news-releases/home-security-systems-market-could-exceed-78-billion-by-2025-301101292.html.

[14] Sumitro Ghatak, Sagar Bose, and Siuli Roy. Intelligent wall mounted wireless fencing system using wireless sensor actuator network. In *2014 ICCCI*, pages 1–5. IEEE, 2014.

[15] Bernhard Groβwindhager, Michael Stocker, Michael Rath, Carlo Alberto Boano, and Kay 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)*, pages 61–72. IEEE, 2019.

[16] Jose A. Gutierrez, Edgar H. Callaway, and Raymond L. Barrett. *IEEE 802.15.4 Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensor Networks*. IEEE, 2003.

[17] Norlezah Hashim and et al. Home security system using zigbee. *Jurnal Teknologi*, 74(10), 2015.

[18] Antonio Ramón Jiménez and Fernando Seco. Comparing decawave and bespoon uwb location systems: Indoor/outdoor performance analysis. In *(IPIN 2016)*, pages 1–8. IEEE, 2016.

[19] Yang Junjie, Lv Jian, and Wei Chunjuan. A wireless solution for substation perimeter safety monitoring system based on zigbee communication technology. In *ICCD 2010*.

[20] KJ Kim. Samsung expects UWB to be one of the next big wireless technologies. https://news.samsung.com/global/samsung-expects-uwb-to-be-one-of-the-next-big-wireless-technologies, 2020.

[21] Andrey Kolmogorov. Sulla determinazione empirica di una lgge di distribuzione. *Inst. Ital. Attuari, Giorn.*, 4:83–91, 1933.

[22] Michael McLaughlin and Billy Verso. Asymmetric double-sided two-way ranging in an uwb communication system, February 14 2016.

[23] Nickolay Smirnov. Table for estimating the goodness of fit of empirical distributions. *The annals of mathematical statistics*, 19(2):279–281, 1948.

[24] Sudeep Tanwar and et al. An advanced internet of thing based security alert system for smart home. In *CITS 2017*.

[25] Al-Khafaji Ahmed Waleed and et al. Iot-based physical security systems: Structures and psmeca analysis. In *IDAACS 2017*, volume 2.

[26] Paul Withington, Herbert Fluhler, and Soumya Nag. Enhancing homeland security with advanced uwb sensors. *Microwave magazine*.

[27] Mingmin Zhao and et al. Through-wall human mesh recovery using radio signals. In *Proceedings of the IEEE/CVF International Conference on Computer Vision*, pages 10113–10122, 2019.