Secure Proximity Detection and Verification

Addressing vulnerabilities in IEEE 802.15.4z UWB

Supervisor: Dr. Mauro Conti
Co-Supervisor: Dr. Chhagan Lal

Vasanth Subramanian

Delft University of Technology

Secure Proximity Detection and Verification

Addressing vulnerabilities in IEEE 802.15.4z UWB

by

Vasanth Subramanian

in partial fulfillment of the requirements for the degree of

Master of Science in Computer Science
Specialization: Cyber Security

at the Delft University of Technology,
to be defended publicly on Monday, October 25th, 2021 at 11:00 AM

Thesis Commitee:	Prof. Dr. Mauro Conti (Supervisor/Chair)	TU Delft, University of Padua
	Prof. Dr. Odette Scharenborg	TU Delft
	Prof. Dr. Apostolis Zarras	TU Delft
Institution:	Technische Universiteit Delft	
Place:	Faculty of Electrical Engineering, Mathematics and Computer Science	

TUDelft

Preface

I would like to express my sincere gratitude to Dr. Mauro Conti and Dr. Chhagan Lal for their invaluable help and guidance throughout the process of my thesis. I also thank the members of the thesis committee, Professor Dr. Mauro Conti, Professor Dr. Odette Scharenborg and Professor Dr. Apostolis Zarras for graciously agreeing to be a part of it. I would like to thank my family and my teachers for their unwavering support.

Vasanth Subramanian
October 2021

Abstract

We live in a world where much of our interactions with the environment around us depend on us being physically close to them. For instance, we have proximity-based tokens (e.g., keys and smartcards) for access systems installed at various places such as in cars, at contactless payment terminals, and in electronic passports. Moreover, such systems exist in critical environments like nuclear power plants. Unfortunately, the current systems used to detect proximity between devices and/or users are rife with vulnerabilities. Numerous attacks, such as Relay attack, Preamble Injection attack, Early Detect/Late Commit, and Cicada, exist that let an attacker maliciously alter the measured distance. The research community has proposed several solutions to address these problems and based on their inputs, the IEEE 802.15.4a standard was recently amended. Nevertheless, we show that the newer amendment (i.e., IEEE 802.15.4z) is however not entirely secure and still vulnerable to being exploited.

In this work, we evaluate and address the vulnerabilities present in the recently introduced standard, IEEE 802.15.4z amendment for Ultra-Wide Band (UWB). This standard forms the basis of proximity detection in a majority of new devices such as keyfobs for cars, access control systems, smartphones like Samsung S21 and Google Pixel 6, and even medical equipment to monitor patients. First, we mount two attacks, namely the Cicada-TF and the Adaptive Injection, against UWB-based proximity detection systems. Second, we propose a novel approach to detect the presence of these attacks. We create a real-world testbed using DWM3000 ICs mounted on NRF52840-devkits to launch the attacks and implement our proposed detection approach. We evaluate the efficacy of our approach in three different environments: an indoor residence, a large outdoor passageway, and an office space. These environments were selected to represent the most commonly used places and were based on the 802.15.4a channel models document by IEEE. Our experiment results show that the proposed model can detect the presence of attacks with high accuracy (94%) in all three environments. To the best of our knowledge, this is the first research work that presents a way to detect the presence of such attacks and also to be verified on hardware.

Contents

Nomenclature

Abbreviations

Abbreviation	Definition
AoA	Angle of Arrival
API	Application Programming Interface
AWGN	Additive White Gaussian Noise
BPM	Burst Position Modulation
BPRF	Base Pulse Repetition Frequency
BPSK	Binary Phase-Shift Keying
CIR	Channel Impulse Response
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator
DRBG	Deterministic Random Bit Generator
ED/LC	Early Detect/Late Commit
ERDEV	Enhanced Ranging Device
ETSI	European Telecommunications Standards Institute
FCC	Federal Communications Commission
FPR	False Positive Rate
FSPL	Free Space Path Loss
GFSK	Gaussian Frequency Shift Keying
GPS	Global Positioning System
HAL	Hardware Abstraction Layer
HPRF	High Pulse Repetition Frequency
HRP	High Repetition Pulse
IC	Integrated Circuit
JSON	Javascript Object Notation
k-NN	K Nearest Neighbours
LoS	Line of Sight
LRP	Low Repetition Pulse
MAC	Medium Access Control
MTAC	Message Time Authenticated Codes
NFC	Near-Field Communication
NIST	National Institute of Standards and Technology
NLoS	Non Line of Sight
OOK	On-Off Keying
PBFSK	Pulsed Binary Frequency Shift Keying
PHR	PHY Header
PHY	Physical Layer
PKES	Passive Keyless Entry System
PPM	Pulse Position Modulation
PRF	Pulse Repetition Frequency
PSR	Preamble Symbol Repetitions
RDEV	Ranging Device
RF	Radio Frequency
RKE	Remote Keyless Entry
RMARKER	Ranging Marker
RSSI	Received Signal Strength Indicator
SDK	Software Development Kit
SDR	Software Defined Radio

Abbreviation	Definition
SFD	Start of Frame Delimiter
SoC	System on Chip
STS	Scrambled Timestamp Sequence
ToA	Time of Arrival
ToF	Time of Flight
UHF	Ultra High Frequency
UWB	Ultra-wide Band

List of Figures

List of Tables

1

Introduction

In this chapter, we provide an introduction to the research topic and the motivation behind our work. We also provide a description of our proposed model and present our major contributions.

We live in a world where we largely interact with the world around us. Noticeably, there has been a strong shift towards contactless systems. Such systems are pervasive in our daily lives. We have proximity based doors, cars that utilize keyless entry systems (where a user does not need to physically open the car door), contactless payment terminals, and even medical devices. Consider a normal example: you go to your neighbourhood grocery store, grab a shopping cart, the doors automatically open to let you in. You finish your shopping, scan your items, and then hold your card near the payment terminal and you have paid for your groceries - no need to enter your pin. You live in the future now, where you do not need to interact with systems. But why stop there? Why do you have to physically bring your card to the payment terminal? Surely we have the technology to eliminate that? Unfortunately, a lot of these systems that we rely upon are based on preexisting technologies that are rife with vulnerabilities and not suitable for such applications.

News articles are peppered with theft reports of cars with keyless systems [1, 37]. Extant solutions use signal characteristics such as Time Of Flight (ToF), Angle of Arrival (AoA), and Received Signal Strength Indicator (RSSI) to measure the proximity between devices and/or users and are susceptible to relay attacks, as shown in Figure 1.1 [21].

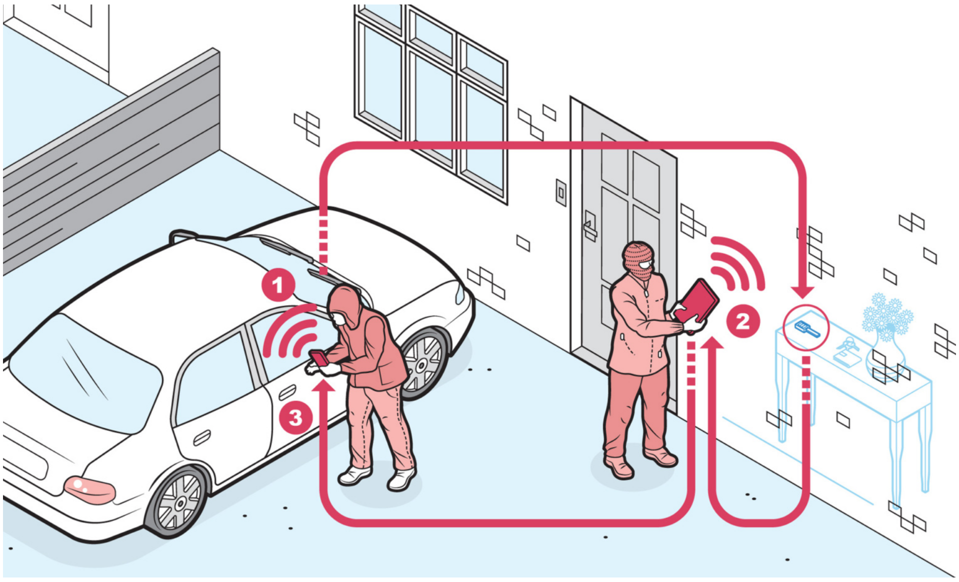


Figure 1.1: Relay attack on Keyless Cars, Image from Which News Co. UK [42]

Relay attacks occur when an attacker who uses a proxy device relays the communication between two devices without necessarily knowing the content of the messages being exchanged. In theft of keyless cars, the hackers first amplify the weak signal from the keyfob present in the house, and then relay it to the car thereby causing the system to unlock. Researchers have also shown such relay attacks being successful on contactless payment systems [16]. There are also other types of attacks that allow the attackers to manipulate the measured distance by utilizing special radio equipment [39]. Recent systems that rely upon the latest Ultra-Wide Band (UWB) standard (IEEE 802.15.4z) are unfortunately also susceptible to similar attacks, namely Cicada++ and Adaptive Injection [47]. In both these attacks, the adversary emits a constant chirp of radio signals that interfere with the genuine signals received by the transmitter, leading to the alteration in the distance measurement. Systems that implement these proximity detection mechanisms hinge their security on weakly transmitted signals and on the notion that encrypted communication implies proximity. The research community has proposed several different methods to combat these problems [46, 48, 32] and an overview of these techniques along with their pros and cons is presented in Chapter 3.

In this thesis, we propose a model to identify the above mentioned new attacks (i.e., Cicada-TF: a modification of the Cicada attack, and Adaptive Injection attack) on the proximity detection systems based on the latest UWB standard. Our proposed model utilizes contextual information and radio signal characteristics that are observed from each ranging session and compares them to historical data that is collected before to identify anomalies that are present.

To summarize, this thesis makes the following contributions:

- We propose an approach that observes and learns the characteristics of genuine ranging sessions. The approach uses these observations, extracts radio signal characteristics and compares them to the earlier recorded datasets of ranging sessions in an environment. We utilize machine learning classifiers that are trained on these recorded datasets to look out for markers of anomalies during subsequent ranging sessions.
- We identify three different real-world environments (Indoor Residence, Outdoor Residence Passageway, and an Office space), where we record the genuine signals at several points within (fingerprint) to accurately account for different variations of ranging that may occur. Our experiments show that our model is capable of identifying Cicada and Adaptive Injection attacks with an accuracy of around 94% in all these environments.
- We mount two attacks on the system to evaluate its efficacy, including a newer attack that is present on the recent IEEE 802.15.4z standard. Furthermore, we evaluate two algorithms namely, Jump-Back Search-Forward and Search-Back [13], proposed by the research community to measure the time-of-arrival (ToA) of received signals. These algorithms are used to account for cases where the strongest signal does not reach the receiver first, such as in Non Line of Sight (NLoS) conditions between the transmitter and receiver. Our results show that Jump-Back Search-Forward algorithm performs consistently better than Search-Back in all three evaluated environments.

In this work, our novel contribution is addressing attacks on proximity detection systems, more specifically on identifying attacks exploiting the vulnerabilities present in the IEEE 802.15.4z standard. Our proposed model does not require special equipment and can be integrated into extant hardware that are built upon the standard.

2 Background

In this chapter, background information on different concepts and techniques that our work relies upon is provided. It includes a short overview on the history of proximity detection systems, basics of Radio Frequency Signal Processing, machine learning concepts, and different secure proximity detection methodologies (i.e., Contextual and Distance Bounding methods). An explanation of the related works that use these methods is provided in the Chapter 3.

Identifying proximity between devices is not a new requirement. The earliest commercial device that implemented a rudimentary form of detecting proximity was a garage door opener with dip switches. The remote (keyfob) for such a system contained a set of 9-12 switches that could be flipped to on/off to set the code that it would transmit. If the switch patterns between the transmitter and the receiver match, the door opens. The transmitted signal was emitted weakly i.e. the transmission energy was limited. This resulted in the signal becoming weak and attenuated over a short distance and hence its range was limited. Such devices did not offer much concerning security as any attacker would be able to brute-force all combinations in a short time. They were also vulnerable to replay attacks, where an attacker could record the signal and replay it later as the content of the signal did not change.

To address the replay attack, newer form of keyless entry systems were introduced that utilize a rolling code, an algorithm which generates a new key each time its used, wherein each transmitted signal is encrypted using a fresh key. These were used in both the traditional Remote Keyless Entry (RKE) systems and the newer Passive Keyless Entry systems (PKES). These keys offered more security as they were not vulnerable to replay attacks, but they were susceptible to newer form of attack called relay attack. In this attack, the adversary establishes a communication channel between the prover (key) and the verifier (car), and subsequently amplifies the power of the emitted signals from the keyfob. This results in the car being able to receive signals from the far away keyfob, and unlocking. The attack is successful due to the fact that the physical distance between the devices is not measured, the system only checks if the car is able to communicate with the keyfob using a challenge-response mechanism. A common PKES protocol is shown in Figure 2.1. The Low Frequency (LF, 125 - 135kHz) waves sent by the vehicle are short range, less than 2 meters, whereas the Ultra-High Frequency (UHF, 315MHz - 433.92MHz) response sent by the keyfob has a range of around 100m [29].

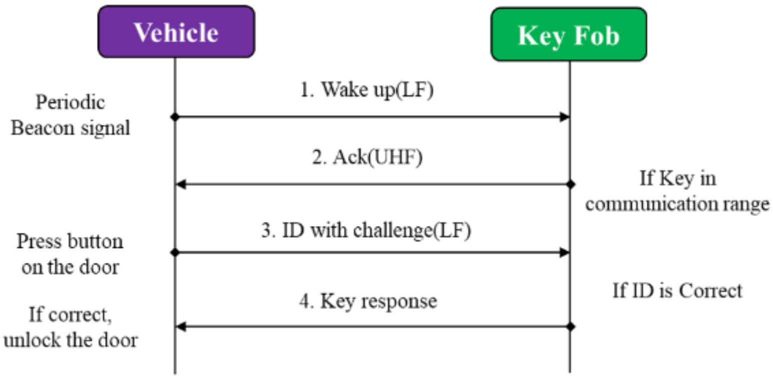


Figure 2.1: Passive Keyless Entry System, Image from Hold the Door! [29]

The research community has proposed several alternate solutions to overcome the above mentioned problems. These solutions can be broadly classified into two categories:

- **Contextual methods**: Here, the devices exchange environmental contexts that they can sense from their surrounding environment, and measure a similarity index to detect if they are in proximity. The context includes radio signals such as WiFi, Bluetooth, and Global Positioning System (GPS), and sensor data like temperature, humidity, light, and pressure.
- **Distance Bounding methods**: Here, the proximity of devices is measured by translating a variety of different parameters such as Time of Flight (ToF), Received Signal Strength (RSS), Angle of Arrival (AoA), and Time Difference of Arrival (TDoA) of the underlying radio signal to distance, and thereby providing a strong upper bound on the distance between two devices.

2.1. Contextual Proximity Detection Methods

Authors in [14] collate a list of several methodologies proposed to detect proximity using contextual information. Commonly used implementations utilize a combination of different sensor's data that can be gathered from the contexts around the transmitter and the receiver. For example, authors in [54] use a combination of different radio signal measurements such as GPS co-ordinates, and list of common WiFi access points read by them, in addition to signal parameters such as RSSI.

Contextual proximity verification schemes, while they boast high accuracies are however susceptible to context manipulating adversaries and can easily be manipulated into verifying devices using off-the-shelf hardware [45, 14]. The adversary can inject radio signals, block signals from the transmitter reaching the receiver, and also perform other context manipulation attacks like altering the environment (e.g., temperature, humidity, and acoustic signals) around the two devices. Also, it does not mathematically guarantee an upper bound on the distances observed between the two devices and as such their security cannot be formally proven. Solutions that attempt to combat context manipulating adversaries utilize machine learning models such as decision classifiers or clustering algorithms to detect anomalous behaviour and prevent relay attacks. Some of these solutions achieve high accuracies [45, 54, 29, 51, 55].

Contextual proximity verification schemes utilize a wide variety of information that can be discerned from the contexts to identify anomalies. They collect information from a wide variety of available different sensor data, and due to the fact that some contextual parameters indirectly impact other parameters of the environment [45], they are useful for detecting the presence of attacks. This is particularly applicable in UWB, as existing systems do not take any contextual information into account. Therefore, we build upon the research work proposed in contextual techniques and adapt them to bolster the security of devices that utilize UWB.

2.2. Distance Bounding Protocols

In distance bounding protocols, a mathematical upper bound on the distances between the two devices is calculated. These protocols were specifically designed to address relay attacks, and are aimed at preventing distance shortening and enlargement attacks. RSS or Phase of Arrival characteristics used to model distances are susceptible to being modified by an attacker without detection [7, 36]. ToF based methods are more secure against these issues (provided the underlying PHY layer does not compromise the security), as an attacker cannot reduce the ToF.

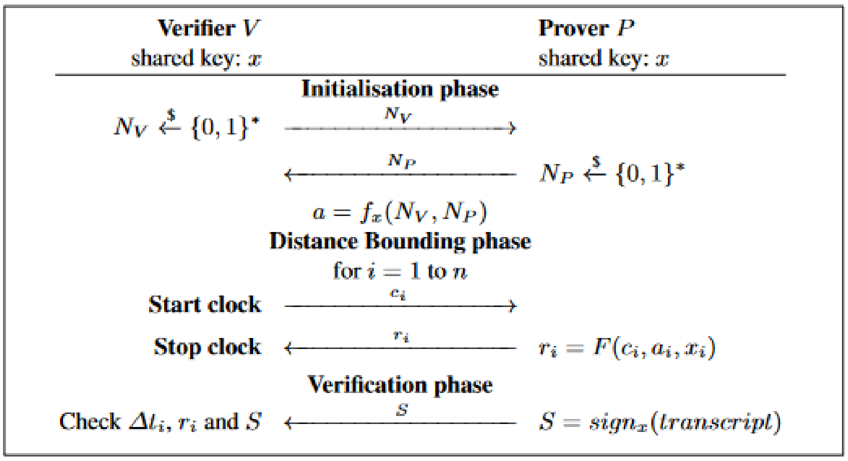


Figure 2.2: Distance Bounding Protocol, Image from [11]

Distance bounding protocols were first proposed by authors in [10]. The design of the protocol outlined by them bounds the distance between the parties by using the round-trip-time (RTT) of single-bit challenges and responses. The protocol runs in three phases. In the first phase, the verifier and the prover exchange their generated nonces followed by the prover committing to a randomly generated string that will be used to calculate responses. In the second phase, also known as the rapid bit exchange phase, the verifier sends “n” single bit challenges to the prover. The prover responds to these challenges by XORing them with the committed string. In the third phase, or the verification phase, the prover signs a message containing the sent challenges and corresponding responses. The verifier utilizes a pseudo-random function to generate the challenges, and the security of the system is directly proportional to the number of rounds. This protocol is shown in Figure 2.2.

While the protocol eliminated the occurrence of relay attacks, newer form of frauds were discovered that were probable depending upon the maliciousness of the different actors involved. Subsequent research work in distance bounding addresses these various concerns and modifies the design of the protocol to address these vulnerabilities [7]. Some common form of fraud outlined are:

1. *Impersonation fraud*: An attacker attempts to convince the verifier that they are legitimate.
2. *Distance Fraud*: A dishonest prover attempts to convince the verifier that they are in the vicinity.
3. *Mafia Fraud*: An attacker launches a man-in-the-middle attack between the verifier and the prover. This is also known as a relay attack.
4. *Terrorist Fraud*: The adversary launches a man-in-the-middle attack and also colludes with a dishonest prover who is located outside the proximity of verifier. The prover actively helps the adversary to maximize the success probability, for example, by providing the nonces used while ensuring that the adversary cannot launch future man-in-the-middle attacks without further help i.e., they do not hand over key material that allow the adversary launch attacks independently.

Distance bounding techniques offer provable security and guarantee an upper bound on the distances between the transmitter and the receiver. Contextual techniques do not offer such solutions. UWB was designed and introduced particularly for the implementation of distance bounding in proximity detection systems to increase their security, as existing devices depended upon non-secure or non-accurate ways to measure distances such as the path loss equation or carrier-phase based ranging. Hence we discuss an overview of existing distance bounding methods and the different threat models that are proposed by the research community.

2.3. Machine Learning Classifiers

Algorithms in machine learning that are capable of identifying different categories in a dataset are referred to as classifiers. In this work, evaluation is done using supervised learning algorithms. In supervised learning, the dataset used to train the model include labels that help them classify or predict data accurately. The model adjusts the weights of the data input to it until it is fitted properly using methods such as cross-validation [18]. These labelled values depict the object’s characteristics and are also referred to as feature values. The training data consists of both inputs and the outputs which allows for continuous learning. Common classification algorithms attempt to recognize entities within the dataset that conform to one pattern, and conclusions are drawn based on these observations.

Some common classification models used are linear classifiers, support vector machines, decision trees, k-nearest neighbours, and random forest. A short description of machine learning models used in this work are presented here. These models were chosen based on the survey of different classification models used in the related works that this work builds upon.

- **Logistic Regression:** It is used to estimate discrete values that are based on a given set of independent variables. It measures the relationship between the dependent variable and the others by estimating the probability of occurrence using its builtin logistics function.
- **K-Nearest Neighbour:** It classifies observations based on their proximity to other points in the data. It works on the presumption that the data points that belong to the same category have characteristics that make them similar. It uses a distance measurement algorithm such as euclidean distance, to measure the proximity to the closest category.
- **Random Forest:** In this, the algorithm creates a collection of decision trees from the dataset. The collection of trees is then merged together to identify the collection with the lowest variance, which results in more accurate data predictions.

Machine learning classifiers are commonly used with large amounts of data, and in this case they are often used in contextual proximity detection methods to identify anomalies and primarily thwart relay attacks. These classifiers are shown to be highly accurate as they build upon genuine datasets collected in the environment, and use them as the basis to detect the veracity of subsequent observations. They are particularly useful in case of UWB, as several important features and signal characteristics can be observed from the radio signals received during ranging. These parameters can then be used for training of the classifier and identification of anomalies.

2.4. Radio Frequency Signal Processing

In this section, we present an overview of fundamentals of radio frequency signal processing. These basic principles are used for the basis for concepts introduced in the later chapters. In wireless communication systems, the typical architecture for a receiver and transmitter is shown in Figure 2.3

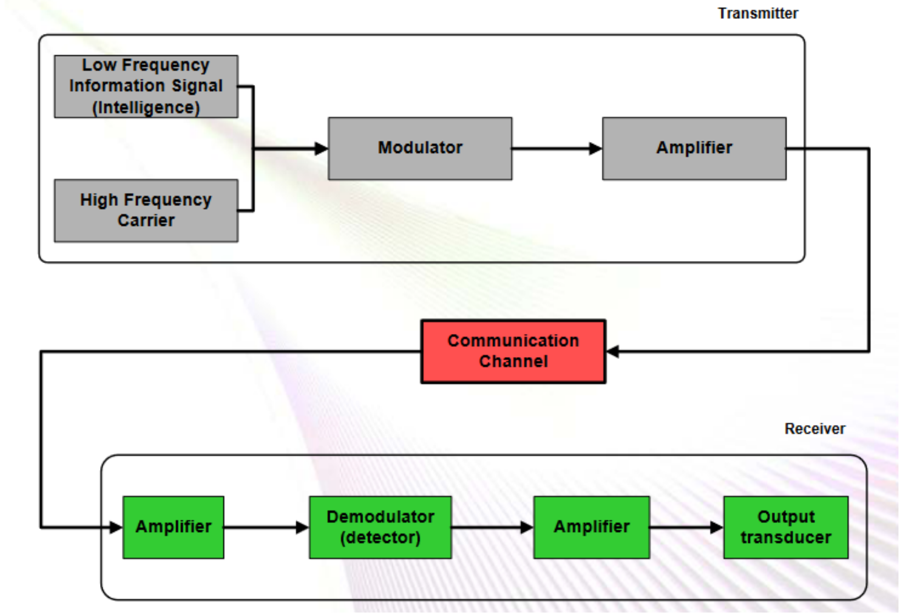


Figure 2.3: Wireless Communication Systems, Image from RF Basics by Texas Instruments

RF signals are electromagnetic radiation waves that are emanated from antennae by an alternating current with a particular frequency. They are mathematically represented by the equation:

$$v(t) = Asin(2 * \pi * f * t + \phi) \tag{2.1}$$

A - amplitude of the signal
f - frequency of the signal
ϕ - phase of the signal

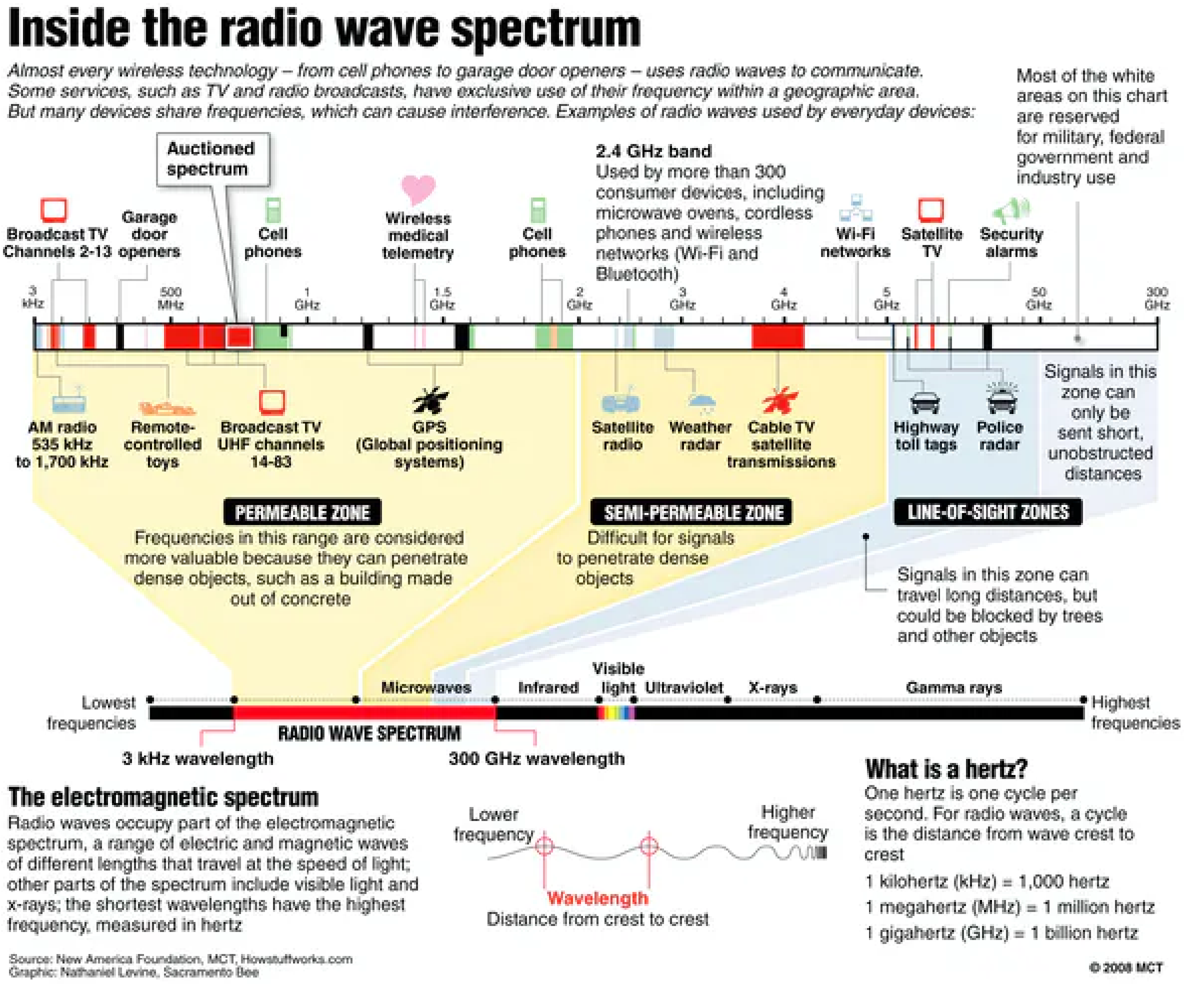
The Wavelength of the signal is given by (λ):

$$\lambda = c/f \tag{2.2}$$

c - the speed of light
f - frequency of the signal

The bandwidth of a signal refers to the frequency range it spans or in other words, the capacity of a link to transmit the maximum amount of data from one point to another over a connection in a given amount of time. For example, Human voice has a bandwidth from 20 Hz to 20 KHz, and 2.4 GHz WiFi has a bandwidth of 22 MHz.

The original data (information signal) that has to be sent wirelessly is referred to as the baseband signal. Usually, a low frequency signal acts as the information signal, that is then converted to a higher frequency before it is propagated over free space. The carrier wave is the signal that is at a steady base frequency (usually higher than baseband), it “carries” the baseband wave to the receiver. The baseband wave is loaded onto the carrier wave using the process of modulation. There are different types of modulation schemes available: Amplitude Modulation, Frequency Modulation, Phase Modulation. The receiver demodulates the observed carrier signal from its antenna to get back the original baseband signal.



Inside the radio wave spectrum

Almost every wireless technology – from cell phones to garage door openers – uses radio waves to communicate. Some services, such as TV and radio broadcasts, have exclusive use of their frequency within a geographic area. But many devices share frequencies, which can cause interference. Examples of radio waves used by everyday devices:

Most of the white areas on this chart are reserved for military, federal government and industry use

2.4 GHz band
Used by more than 300 consumer devices, including microwave ovens, cordless phones and wireless networks (Wi-Fi and Bluetooth)

PERMEABLE ZONE
Frequencies in this range are considered more valuable because they can penetrate dense objects, such as a building made out of concrete

SEMI-PERMEABLE ZONE
Difficult for signals to penetrate dense objects

LINE-OF-SIGHT ZONES
Signals in this zone can only be sent short, unobstructed distances

Signals in this zone can travel long distances, but could be blocked by trees and other objects

The electromagnetic spectrum
Radio waves occupy part of the electromagnetic spectrum, a range of electric and magnetic waves of different lengths that travel at the speed of light; other parts of the spectrum include visible light and x-rays; the shortest wavelengths have the highest frequency, measured in hertz

What is a hertz?
One hertz is one cycle per second. For radio waves, a cycle is the distance from wave crest to crest

1 kilohertz (kHz) = 1,000 hertz
1 megahertz (MHz) = 1 million hertz
1 gigahertz (GHz) = 1 billion hertz

Wavelength
Distance from crest to crest

Source: New America Foundation, MCT, Howstuffworks.com
Graphic: Nathaniel Levine, Sacramento Bee

© 2008 MCT

Figure 2.4: Inside the Radio wave spectrum, Image from New America foundation

The energy of radio signals attenuates as it propagates through free space, this loss in energy is proportional to the square of the distance travelled. It can be mathematically represented by the Friis Free Space Path Loss (FSPL) equation. The behaviour of these waves as they propagate in space depends on the frequency of the carrier wave. For example, radio waves in 2.4 GHz can pass through people and smaller rooms in buildings easily, but UWB waves in 8GHz spectrum are impacted more strongly by reflections and obstacles. Figure 2.4 shows the radio wave spectrum and the behaviour of waves at different frequencies.

$$FSPL = (4dfc)^2 \tag{2.3}$$

c - the speed of light
f - frequency of signal
d - the distance travelled by signal

When the receiver and the transmitter have a clear line of communication, its referred to as Line of Sight (LoS). When there are obstructions or obstacles between the path of the transmitter and receiver, its referred to as Non Line of Sight (NLoS).

3

Related Work

In this chapter, we present a detailed discussion on the related work that form the basis of our proposed approach. These research articles can be classified broadly into two categories, context-based and distance bounding-based secure proximity detection techniques.

3.1. Contextual Proximity Detection

In [45], the authors evaluate the security of contextual proximity detection methods against context manipulating adversaries. They highlight the weakness of systems that rely solely on such contexts, and present a decision classifier that is trained on and utilizes all the individual sensors available to identify potential anomalies. When relying upon multiple sensors, their machine learning based approach achieves higher resistance to attacks. They mount relay attacks against their system and evaluate the efficacy of their machine learning model using different combinations of available sensor data. While their solution achieves good accuracies, they do not completely test their model against stronger context manipulating adversaries. Such adversaries can influence several, if not all the used contexts around the environments, and can falsely convince the system into classifying the malicious ranging sessions as legitimate. A ranging session is defined as the set of messages the transmitter and the receiver exchange, that lets them measure the distance between them.

In [51], the authors present a similar multi-modal decisions-fusion classifier that relies on multiple sensors to achieve high accuracies against relay attacks. However, both these methods do not provide a strong upper bound on distances. Authors in [54] provide another context based machine learning approach that utilizes multiple sensors available and a decision tree classifier to achieve high accuracies with low False Positive Rate (FPR). The authors train the classifier using normal use-cases and mount attacks to simulate abnormal ones. However, they also acknowledge that an adversary that can manipulate a larger majority of the sensors can circumvent the system, and hence their proposed model has the same vulnerabilities as the one proposed by authors in [45].

In [29], the authors implement a RF fingerprinting method that can be trained to identify legitimate and malicious key attempts in PKES and RKES. They utilize a k-NN (K Nearest Neighbours) classifier that is initially trained using legitimate keyfobs, and then they mount several attacks such as relay attacks, amplification attacks, battery aging and temperature variation attacks by context manipulating adversaries, against it to test its efficacy. Authors also claim high accuracies with low FPRs with sufficiently larger training dataset. The authors however acknowledge that relay attacks are possible with sufficient equipment and do not offer a clear upper bound on distances. The general consensus amongst them is that contextual multi-modal techniques are more accurate i.e., higher the number of the contexts being taken into account, better the accuracies of the classifiers at detecting anomalies. However, just increasing the number of sensors that the machine learning classifier considers introduces several limitations. Firstly, each device used for ranging must possess all the sensors that are being taken in consideration leading to the increase in costs per device. Secondly, increasing the number of features may lead to the problem of over-fitting where the classifier incorrectly depends on very specific values of the features used. This can be alleviated by utilizing larger datasets. Thirdly, utilizing many sensors adds severe latency to the processing overhead. Since the devices utilized for ranging must be highly accurate (in the order of nanoseconds), dependence on several sensors may lead to a drop in accuracy.

Biometric contexts, on the other hand, while being more accurate and resistant to context manipulating adversaries, are however more expensive to accurately measure. For example, estimating gait biometrics requires the presence of multiple sensors and/or devices mounted upon the user [30, 43, 44]. In these research works, the proposed models take different biometric contexts into account such as the path a transmitter takes when a ranging session is performed and/or the gait biometrics of the user (the one possessing the transmitter).

Other contextual proximity schemes rely upon audio to verify location [52, 56]. In [51], the authors use audio signals to measure the room impulse response of the surroundings of the prover and verifier by sending an audio signal, and comparing the echos received by both devices. They achieve high accuracies with low FPR, but they do not evaluate their model against active adversaries who can manipulate the audio signals around the devices.

In [56], the authors propose a two factor authentication scheme that utilizes audio signals and is resistant to co-location and relay attacks. In both the proposed models, the authors do not evaluate the security against context manipulating adversaries. Such an adversary can inhibit the working of their system by flooding the environment with ultrasonic sound signals that interfere with the genuine ranging sessions. This causes the same “echo” to be observed by both the transmitter and the receiver, leading to malicious ranging sessions succeeding.

In summary, contextual proximity techniques utilize a wide variety of sensor data gathered from the environment around the devices which can be used for the identification of anomalies during ranging sessions. However the security of such systems are not provable, as they are susceptible to context manipulating adversaries. Additionally, they also do not measure the distances between the transmitter and receiver and thus do not guarantee an upper bound. The model proposed in this thesis addresses these concerns, as it offers a strong upper bound on the measured distances in addition to utilizing the available context information around the transmitter and the receiver to look for anomalies.

3.2. Distance Bounding

Extant distance bounding methodologies that provably guarantee upper bounds on the distances require the use of specialized hardware, i.e., hardware that is designed to be accurate at measuring time in the order of nanoseconds. Such specialised hardware also have low level access to the radio hardware to minimise processing time while communicating with other devices. An upper bound of 15cm on the distances observed require that devices be able to receive, process, and transmit signals in less than 1 ns [41, 40, 2, 17, 53]. For example, in Android devices, access to the low-level hardware is provided by the Hardware Abstraction Layer (HAL) which interacts with android's Linux kernel and acts as a general interface to the low-level drivers of the sensors. Due to the abstraction of the lower layers, the usage of higher layer APIs (Application Programming Interfaces) increase the latency and thereby the processing times when being leveraged. Therefore, it corresponds to an increase in the upper bound offered. This increase in the processing delay introduced is observed, especially when utilizing the abstracted NFC stack that android offers in the proof-of-concept implementation of the Swiss-Knife distance bounding protocol in an android smartphone [23, 31]. The processing duration after all the abstractions introduced by the android stack results in a latency of 1.4 ms, which results in an upper bound of 300 Kms.

Minimizing the advantage for the adversaries under different threat models while achieving low space and time complexities is a major focus for the upcoming distance bounding protocols, which already guarantee security against distance fraud and mafia fraud at the logical layers, with the recent methodologies also offering security against distance hijacking and terrorist fraud [7]. In this work, the authors present a survey of all proposed distance bounding authentication schemes. They compare and contrast these distance bounding techniques in terms of security against different threat models, the processing overhead incurred and the success rates of an adversary mounting attacks. These systems are being widely implemented in UWB based radio peripherals, these hardware primarily utilize the UWB to send their radio signals and measure distance using ToF as opposed to RSS. These devices although in existence since 2003 [4] were quite expensive and thus found usage only in certain conditions despite their potential pervasive applications. However, the availability of these devices or chipsets are now increasingly becoming more common, with them now being included in off-the-shelf mobile devices. Major device manufacturers include these UWB chipsets in their devices and operating systems such as Android [5], and iOS [6] also have added API support to leverage UWB chips.

Protocols such as WiFi, NFC (Near-Field Communication), and PKES have underlying security vulnerabilities that make it possible for an attacker to circumvent the bounded distances by exploiting the PHY layer to perform relay attacks [33, 19, 21, 22]. Currently, such systems are implemented using the UWB protocol, which was designed in consideration of such vulnerabilities. Unfortunately, similar attacks that attempt to decrease or increase the measured distance exist even in UWB-based methodologies [13, 48] where it is prone to attacks such as Cicada, and Early Detect/Late Commit (ED/LC) [38]. These attacks exploit the predictable nature of the symbols used in the frames exchanged during ranging i.e., the messages that are sent by a genuine transmitter to synchronise with the receiver are made of up publicly known sequences leading to an adversary who can manipulate the measured distances using sufficient radio equipment. However, UWB can be modified to account for such attacks, authors in [46] use pulse reordering and cryptographic pulse blinding to prevent mafia-fraud like attacks at the physical layer, and in [48], they provide a way to detect distance enlargement attacks. Both these solutions attempt to solve the vulnerabilities that existed in the IEEE 802.11.4a standard for UWB.

The revised and updated standard namely 802.11.4z now includes inbuilt protection against Cicada and ED/LC attacks in the form of Scrambled Timestamp Sequence (STS). While they greatly increase security against such attacks, their security is not formally defined. Other methods such as Message Time Authenticated Codes (MTACs) have been proposed by the research community, to preserve the integrity of message arrival times where the receiver can cryptographically check the consistency of modulation [32]. Recently, in [47], authors present a security analysis of the IEEE 802.15.4z UWB HRP

(High Rate Pulse) PHY layer, specifically the High Pulse Repetition Frequency (HPRF) standard. They introduce two new advanced attacks, Cicada++ and Adaptive Injection Attack and evaluate the security with regards to the success rates of the attacker. They show that depending upon the threshold parameters selected, an attacker will be able to gain up to 25% success rates when injecting signals. They perform experiments of the proposed attacks using simulations in Matlab and evaluate the performances in different environments. The environments chosen for simulations are chosen based on the IEEE channel models document. This document contains assessments and models of the behaviour of UWB waves in a variety of several common environments where such systems might find applications in. Details about the original standard, the amendment, and vulnerabilities that exist in them are elaborated upon in Chapter 4.

In summary, the current UWB standard used in devices for proximity detection has several vulnerabilities present. The research community has proposed several solutions to combat these problems, but the latest IEEE standard designed specifically around these considerations, does not yet fully solve the security concerns. This work is motivated by these concerns and we present a solution to identify and mitigate the occurrence of such attacks by considering the contextual channel information. This is in contrast to extant methods, where the time of flight algorithm does not consider the environment characteristics into account when identifying the first path.

4

Ultra-Wide Band

In this chapter, we provide an overview of the Ultra-Wide Band standard as defined by the IEEE working group. This group was established primarily to create a new protocol that was aimed at low-rate wireless devices with limited battery capacities to achieve proximity detection. We discuss the symbol structure, the frame format, the types of UWB standards, and also their security implications. We then present an overview of the different vulnerabilities that exist in these standards, and the amendments that were proposed to address them.

4.1. Design of Ultra-Wide Band

The design of UWB was to enable low-rate communication (IEEE 802.15.4) between devices in close proximity to each other, under the umbrella of wireless personal area networks (IEEE 802.15 PAN). The IEEE 802.15.4 standard documents and describes the Physical Layer (PHY) and the Medium Access Control (MAC) sublayer. More specifically, it was introduced to address the need to communicate with portable, low-powered devices with limited or no-battery capacity and also enable precision ranging. And as such, the design and regulations of the transmitted carrier wave have been modelled after these considerations.

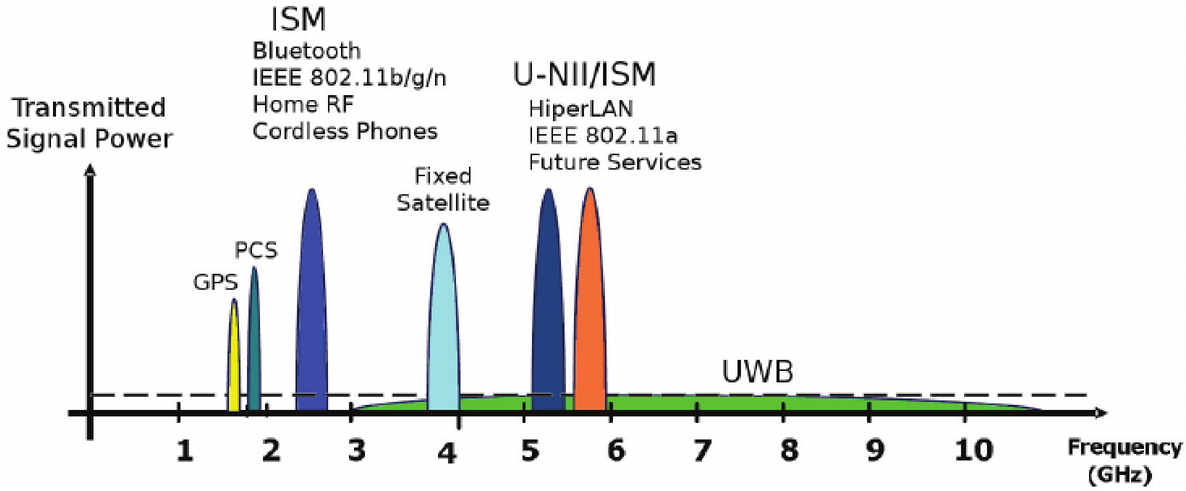


Figure 4.1: Spectral Density of common Radio Signal Protocols, Image from [25]

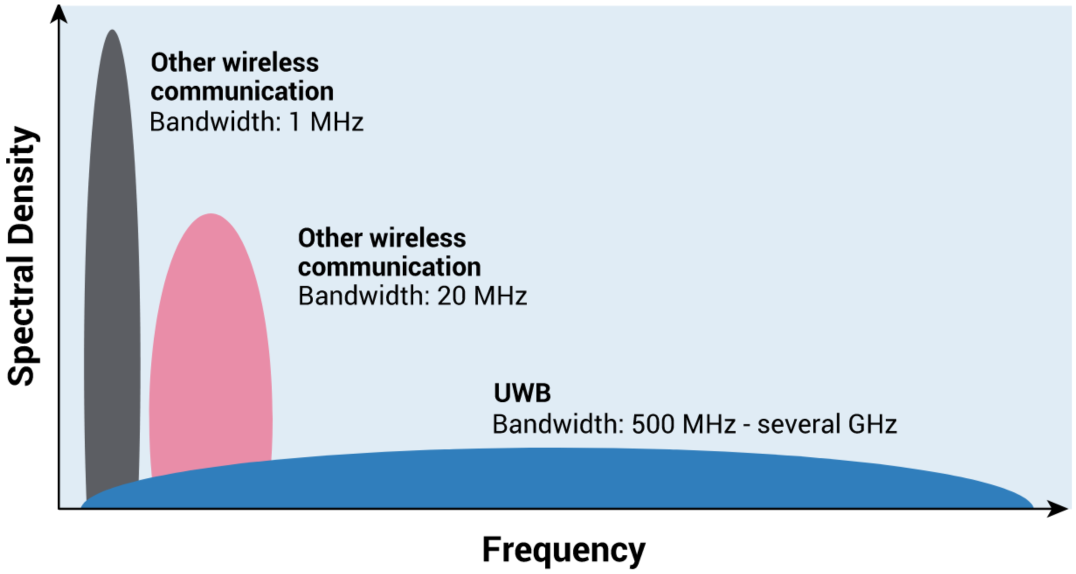


Figure 4.2: Spectral Density of common Radio Signal Protocols, Image from Fira Consortium

UWB signals are defined as radio signals with an instantaneous bandwidth that is larger than 500 MHz or with a fractional bandwidth that is larger than 20% [57]. The signal power parameters are dictated by FCC (Federal Communications Commission) and ETSI (European Telecommunications Standards Institute) regulations which dedicate certain bands of frequencies for specific applications.

GPS, Bluetooth, Cordless phones, Wifi (2.4 and 5.0 GHz) and other commercial radio devices are confined to specific frequencies, within which all transmission must occur.

Radio technologies such as Bluetooth and WiFi aren't regulated on their transmitted RF energy, and thus are suitable for continuous high data rate communications. However, the transmission of UWB is limited strictly by the regulations and must adhere mainly to the following:

1. The mean Power Spectral Density, i.e., the radiated power of the signal within a given bandwidth, must not exceed $PSD = -41.3dBm/Hz$ when averaged over the duration of 1ms.
2. The power of each individual pulse must not exceed $0dBm$ when the signal is passed through a $50MHz$ bandwidth filter.

The spreading of the signal over a larger bandwidth results in lesser interference with other existing signals that occupy the same band. Thus having stronger resistance to impacts from multipath in addition to having time domain resolution characteristics that enable accurate positioning and tracking of the device [57]. The UWB used in IEEE 802.15.4 standard is also called impulse radio UWB because it is based on pulses of RF energy.The two regulations mentioned above for UWB may be inferred as a bucket of power that is available to be distributed, either in a few pulses (LRP, Low Rate Pulse) or split over several pulses (HRP, High Rate Pulse). The number of transmitted pulses in HRP UWB is more than in LRP UWB, but the individual pulse energy is proportionally weaker. Both LRP and HRP use exactly the same transmitted RF energy. The number of pulses in 1ms is referred to as the pulse repetition frequency (PRF). Correspondingly, depending on the PRF, UWB is split into LRP and HRP.

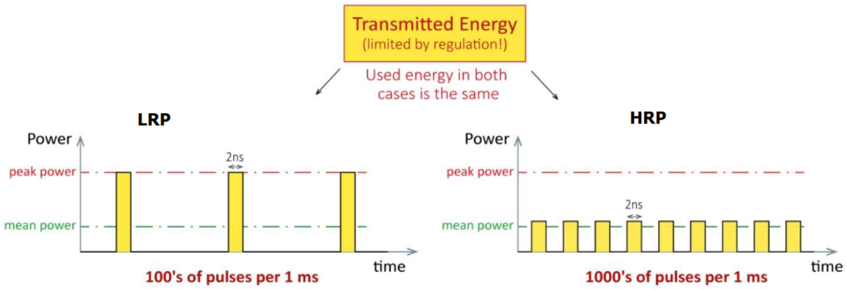


Figure 4.3: Difference between LRP and HRP, Image from [3]

The frequency spectrum allocated to UWB extends from 3.1 GHz to 10.6 GHz, with the allocated spectrum split into 15 channels, and an additional channel allocated under the sub-GHz spectrum with the same bandwidth of 499.2 MHz (referred to as channel 0). The channel allocations for UWB are shown in Figure 4.4, the x axis indicates the centre frequency of the channel.

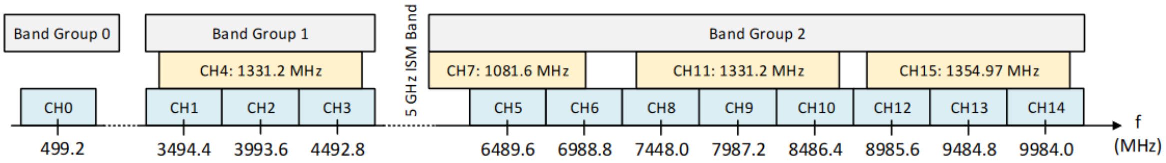


Figure 4.4: Band allocation for UWB, Image from Fira Consortium [27]

Owing to the multitude of research that corroborates that UWB is a major enabling technology for low powered sensor network devices, capable of locating and tracking of objects[49], surveillance [24], localization [20], and other proximity based interactions, the IEEE established a dedicated standardization committee IEEE 802.15.4a to design a PHY layer that accommodates these requirements [12]. This standard defines the underlying PHY layer for HRP. LRP was introduced in an amendment later called 802.15.4f.

The introduced PHY layer divides the spectrum into following three individual bands:

1. Band 0 - Sub-gigahertz channel

2. Band 1 - Low-band HRP UWB channels
3. Band 2 - High-band HRP UWB channels

The use of a larger bandwidth allows for a longer range of communication and enhances the multi-path resistance leading to more accurate measurements. The frequency gap between Band Group 1 and Band Group 2 was introduced to avoid interference between UWB and technologies in the 5 GHz ISM band [27].

4.2. Characteristics of a UWB wave and IEEE frame structures

UWB systems are expected to be used in a multitude of different environments such as residential, office, industrial, and outdoor areas. Such complex environments lead to a large degree of signal reflection and diffraction. The signal undergoes all these reflections, diffraction, and attenuation and when it arrives at the antenna of the receiver, it is a combination of weakened, delayed, and overlapping versions of the original signal [27]. All these parts of the signal are called as multi-path components. In the event of Non Line of Sight (NLoS), it is also possible that the strongest signal does not reach the receiver first, and the antenna observes a weaker attenuated signal. This can be observed in Figure 4.5.

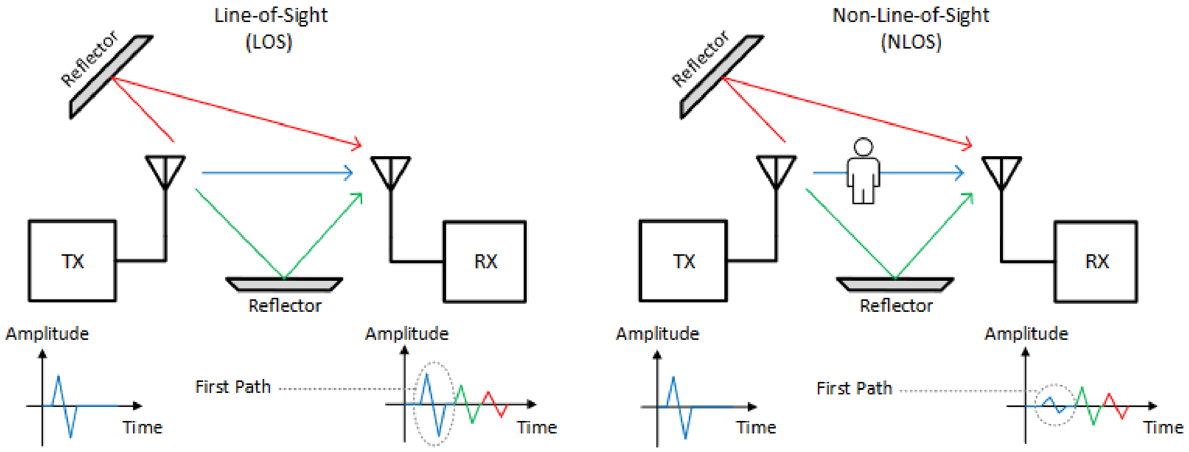


Figure 4.5: Effects of Line of Sight on UWB and Non Line of Sight, Image from Fira Consortium [27]

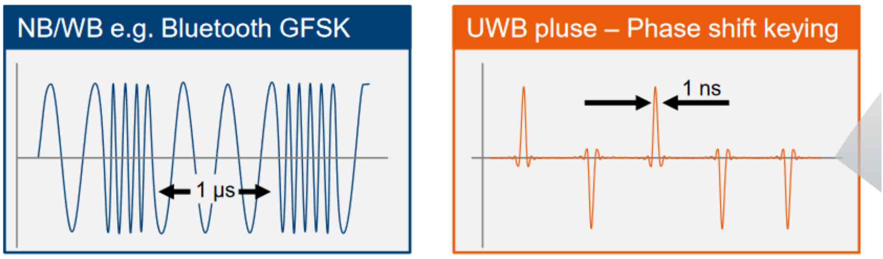


Figure 4.6: Difference between modulation in Bluetooth and UWB, Image from Rohde&Schwarz webinar: Second life of UWB

UWB utilizes a modulation scheme that is much different to that of conventional schemes. For example, Bluetooth utilizes a Gaussian Frequency Shift Keying (GFSK) mechanism where it passes the data pulses through a Gaussian filter to make the transitions smoother in the narrow band where the signals are transmitted. The channel bandwidth is around 22 MHz. UWB, on the contrary, encodes the bits onto the carrier wave using a phase shift keying modulation (mode of operation dependent) scheme, with each bit being sent as a symbol or a group of symbols using pulses of radio waves. These pulses of waves spread the symbols over time, and due to the transitions being much clearer, the amount of inter-symbol interference is reduced. This lets the receiver observe and resolve the ToA of these symbols clearly.

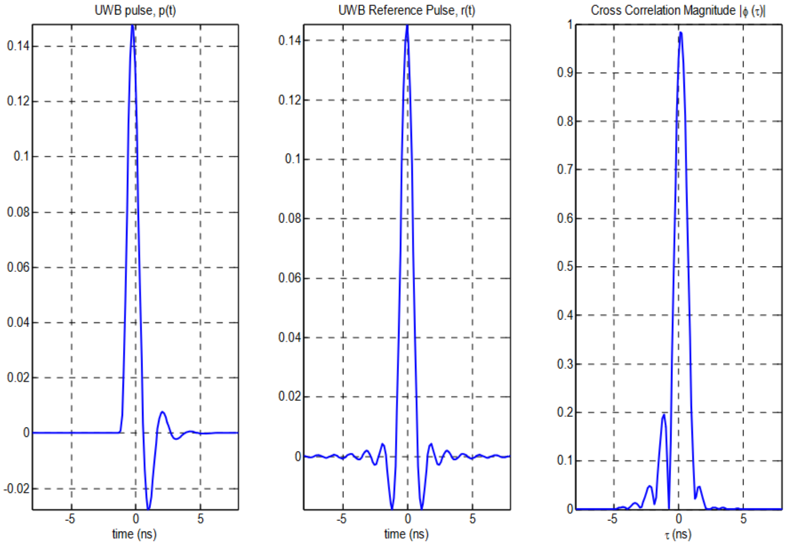
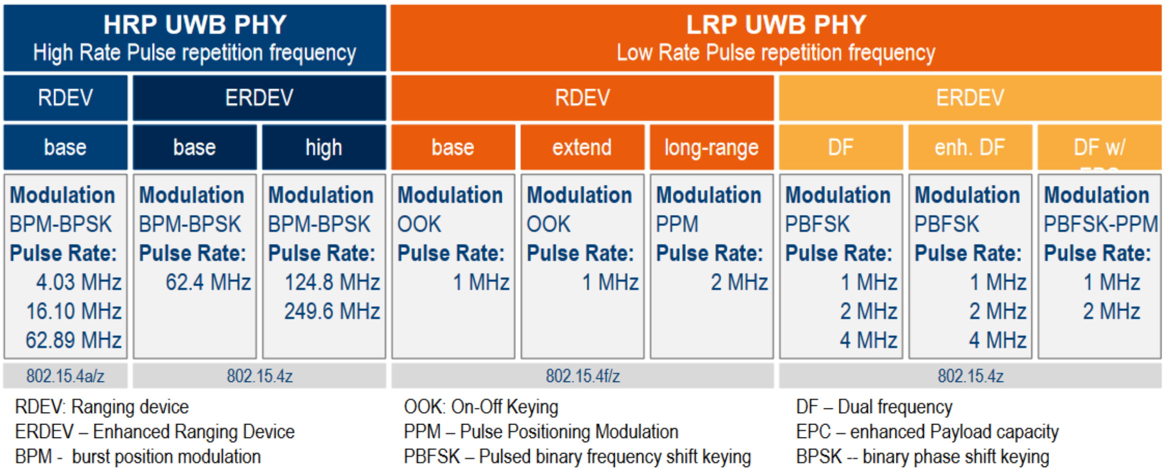


Figure 4.7: A UWB (Channel 9) compliant transmitted pulse (left), reference pulse (middle), magnitude of cross-correlation (right), Image from IEEE 802.15.4 standard [26]

The IEEE 802.15.4 standard defines a reference UWB pulse as a root-raised-cosine pulse with a roll-off factor of $= 0.5$. The transmitted pulse shape $p(t)$ is constrained by the shape of its cross-correlation function with a standard reference pulse, $r(t)$. LRP pulses contain more energy but are fewer in number, whereas HRP pulses are weakly powered but with a substantially larger number of pulses. Over long distances, the receiver will be unable to see the individual pulses, in contrast to HRP where the energy of the pulses is accumulated. This makes HRP resistant to attenuation over long distances and extends range in addition to having higher data-rate capabilities.

Since the LRP's individual pulses contain more power, the individual bits are encoded as single pulses. However, to account for the larger number of pulses, the HRP mode encodes each bit into several pulses, or symbols. In other words, LRP utilizes short symbols whereas HRP utilizes multiple symbols to represent each bit. This has multiple security implications on distance bounding, explained in Section 4.2.1. Figure 4.8 refers to the different types of UWB PHY outlined by the IEEE standards.



HRP UWB PHY High Rate Pulse repetition frequency			**LRP UWB PHY** Low Rate Pulse repetition frequency					
RDEV	ERDEV		RDEV			ERDEV		
base	base	high	base	extend	long-range	DF	enh. DF	DF w/
Modulation BPM-BPSK	**Modulation** BPM-BPSK	**Modulation** BPM-BPSK	**Modulation** OOK	**Modulation** OOK	**Modulation** PPM	**Modulation** PBFSK	**Modulation** PBFSK	**Modulation** PBFSK-PPM
Pulse Rate: 4.03 MHz 16.10 MHz 62.89 MHz	**Pulse Rate:** 62.4 MHz	**Pulse Rate:** 124.8 MHz 249.6 MHz	**Pulse Rate:** 1 MHz	**Pulse Rate:** 1 MHz	**Pulse Rate:** 2 MHz	**Pulse Rate:** 1 MHz 2 MHz 4 MHz	**Pulse Rate:** 1 MHz 2 MHz 4 MHz	**Pulse Rate:** 1 MHz 2 MHz
802.15.4a/z	802.15.4z		802.15.4f/z			802.15.4z		

RDEV: Ranging device
ERDEV – Enhanced Ranging Device
BPM - burst position modulation

OOK: On-Off Keying
PPM – Pulse Positioning Modulation
PBFSK – Pulsed binary frequency shift keying

DF – Dual frequency
EPC – enhanced Payload capacity
BPSK -- binary phase shift keying

Figure 4.8: Flavors of UWB 802.15.4, Image from Rohde&Schwarz

Each of the two UWB PHY specifications are further grouped under RDEV (Ranging Device) or

Enhanced Ranging Device (ERDEV). The RDEV specifications were introduced in the 802.15.4a, with a newer specification outlined more recently for ERDEV in the 802.15.4z amendment. Details of this amendment are discussed in Section 4.4. ERDEV devices are capable of more accuracy, and primarily introduced to address security concerns that were present on ranging devices.

4.2.1. Low Rate Pulse

In Low Rate Pulse, support is provided for three transmission modes, each addressing a specific need.

1. Base mode for the highest data rate.
2. Extended mode for moderate data rate, but for improved sensitivity.
3. Long-range mode for the highest sensitivity.

A combination of On-Off Keying (OOK) modulation or Pulse Position Modulation (PPM) or Pulsed Binary Frequency Shift Keying (PBFSK) is used to modulate the symbols. The individual bits are represented by either 1, 4, or 16 symbols depending upon the transmission mode selected. A symbol in base mode of transmission is shown in Figure 4.9. Due to the large spacing between each pulse, any reflections caused fade out before the arrival of the subsequent pulse. This allows for the simple and efficient processing of the incoming pulses to derive the ToA in ranging and data decoding.

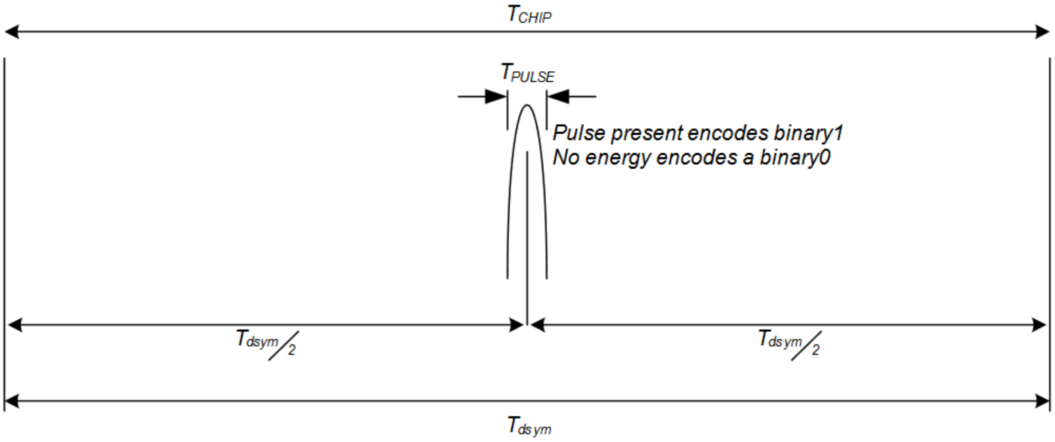


Figure 4.9: Base mode LRP UWB PHY symbol structure, Image from IEEE 802.15.4 standards [26]

Security of LRP

The security of LRP is dependent on provably-secure primitives. These systems use authenticated distance bounding protocols and commitment schemes that are formally proven to be resilient against strong attackers [8, 50]. This is owing to the usage of short symbol sizes that prevents the attacker from exploiting vulnerabilities which are present in the 802.15.4 standard. An overview of these vulnerabilities is given in Section 4.3. In this work, we evaluate the security of the UWB HRP PHY and focus on its vulnerabilities, and therefore will elaborate further on that specification.

4.2.2. High Rate Pulse

The HRP UWB PHY uses a combination of both Burst Position Modulation (BPM) and Binary Phase-Shift Keying (PBSK) to modulate the signals. In this modulation scheme, each symbol can be used to encode two bits of information. Each symbol consists of a group of consecutive chips called a burst. The position of these bursts in the first or second half of the symbol duration denotes a single bit as shown in Figure 4.10. The first bit is used to determine the position of a burst of pulses, and the second bit is used to modulate the phase i.e., the polarity of the signal in this burst.

UWB communications are based on the transmission and reception of frames. Figure 4.11 shows the general structure of the UWB frame. It begins with a synchronization header consisting of the preamble and the Start of the Frame Delimiter (SFD), after which the PHY Header (PHR) defines the

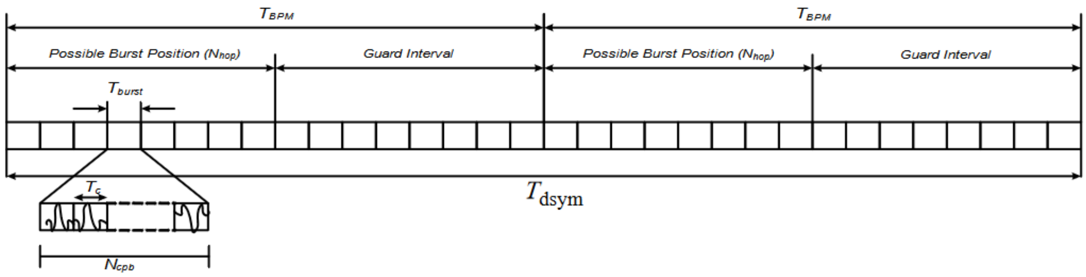

T_BPM
T_BPM
Possible Burst Position (N_hop)
Guard Interval
Possible Burst Position (N_hop)
Guard Interval
T_burst
T_c
T_dsym
N_cpb

Figure 4.10: Base mode HRP UWB PHY symbol structure, Image from IEEE 802.15.4 standards [26]

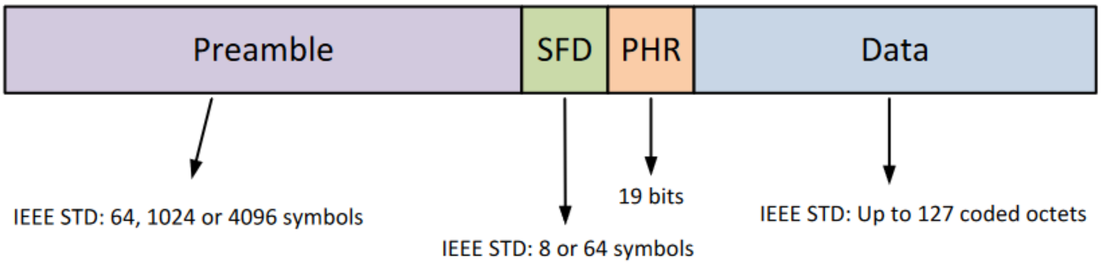

Preamble
SFD
PHR
Data
IEEE STD: 64, 1024 or 4096 symbols
IEEE STD: 8 or 64 symbols
19 bits
IEEE STD: Up to 127 coded octets

Figure 4.11: UWB 802.15.4a UWB HRP Frame Format, Image from Decawave User Manual [17]

length and data rate of the data payload part of the frame [17]. The Synchronisation Header (SHR) consists of the preamble and the Start of Frame Delimiter (SFD). The SHR is made up of single pulses as opposed to the BPM/BPSK modulations used for the PHR and data. The symbol is divided into approximately 500 “chip” time intervals, in which either a negative or a positive pulse may be sent, or no pulse. The “chip” interval is 499.2 MHz which is a fundamental frequency within the UWB PHY [17]. The sequence of pulses sent during the preamble symbol interval is determined by the preamble code. The standard defines 8 preamble codes of length-31 for use at 16 MHz PRF and 16 preamble codes of length-127 for use at 64 MHz PRF. The preamble length and duration is defined by the number of Preamble Symbol Repetitions (PSR) and it has four settings: 16, 64, 1024, and 4096.

The length-31 codes are spread by inserting 15 zeros after each pulse to give the 496 chip times per symbol while the length-127 codes are spread by inserting 3 zeros after each pulse to give the 508 chip times per symbol. The SFD signals the end of the preamble and the beginning of the PHY header [17]. The preamble sequence has a property of perfect periodic auto-correlation [28] which in essence allows a coherent receiver, a receiver that tracks both phase and time of the carrier wave, to determine the exact impulse response of the RF channel between transmitter and receiver [27].

The Channel Impulse Response (CIR) is a measure of all the aggregated radio signal energies received over time. These aggregated signals, which may include early path and/or multi-path components, are then correlated with a locally stored template to measure the similarity. This measure of the correlated signal over time, as it includes the measure of these different components, may be construed as an echo-gram of the environment around the antenna [27, 35]. ToF ranging systems are very sensitive to the exact time of arrival of the signal, as each nanosecond causes an accuracy drop of 30cm. In NLoS conditions, the first path component of received signals needs to be identified so that the exact ToA may be calculated. For this purpose, leading edge algorithms are utilized.

There are two types of leading edge algorithms proposed by the research community, namely Jump-Back Search-Forward and Search-Back as shown in figures 4.12 and 4.13. The two algorithms differ in the way they operate. In Jump-Back Search-Forward, the algorithm jumps back by a set time-window from the correlated highest peak observed in the CIR. It then searches forward for the first occurrence of a peak that is above the noise threshold that is present before the highest peak. This is identified as the first path of component of the signal. In Search-Back, the algorithm searches continuously backwards from the highest correlated peak and identifies the first peak that occurs before the algorithm reaches a noise-only region.

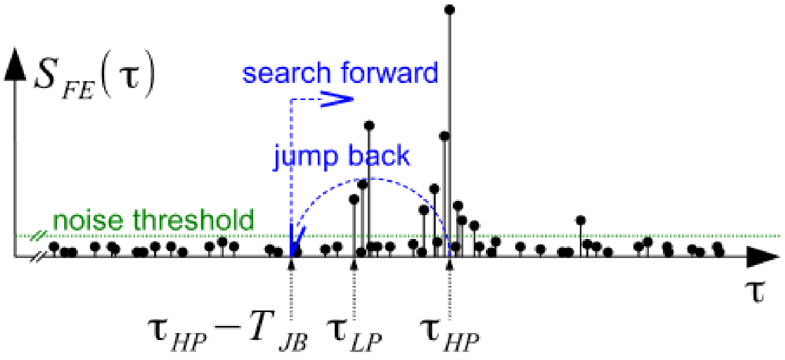


Figure 4.12: Jump-Back Search-Forward Leading Edge Detection Algorithm, Image from [13]

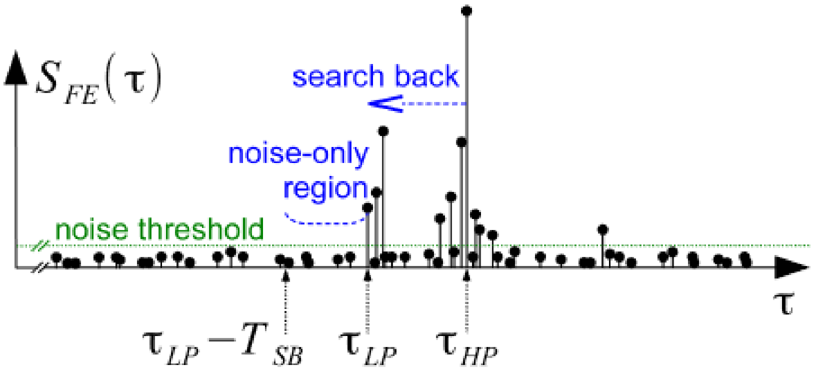


Figure 4.13: Search-Back Leading Edge Detection Algorithm, Image from [13]

4.3. Security of 802.15.4a UWB HRP

Due to the usage of large symbol sizes for each bit representation, distance bounding methods as described in Chapter 3 are not suitable. It is due to their susceptibility of being identified using the initial few symbols for a given bit. This leads to the compromise of the protocol, although it offers mathematical bounds on security, it cannot be utilized if the underlying physical layer is inherently susceptible to vulnerabilities. This enables the attacker to sniff the bits being sent during the rapid bit exchange phase and committing them earlier than when the original signal reaches. Thus leading to the alteration of the time of commitment.

In [38], the authors show an attacker who could decrease the measured distance by more than 130m due to the predictable nature of the preamble and the payload data with extremely high accuracy (99%). The attacker need not wait for the entire symbol to be transmitted as just knowing the initial parts lets them guess the rest, and inject it in a way that the entire symbol reaches the genuine receiver sooner than this.

In [13], the authors present a new vulnerability called Overshadowing attack where the attacker inserts a larger peak, after the original peak present in the CIR. This lets an attacker effectively convince the leading edge algorithm implemented by the receiver to choose the original peak as the first path depending upon the leading edge algorithm used. This attack can be observed in Figure 4.14.

In [38], the authors present cicada attacks against UWB IEEE 802.15.4a. In this attack, the adversary emits a periodic chirp of pulses with a higher power during the transmission of the preamble. When these chirps coincide with the signal, there is a peak observed in the side lobes of the signal

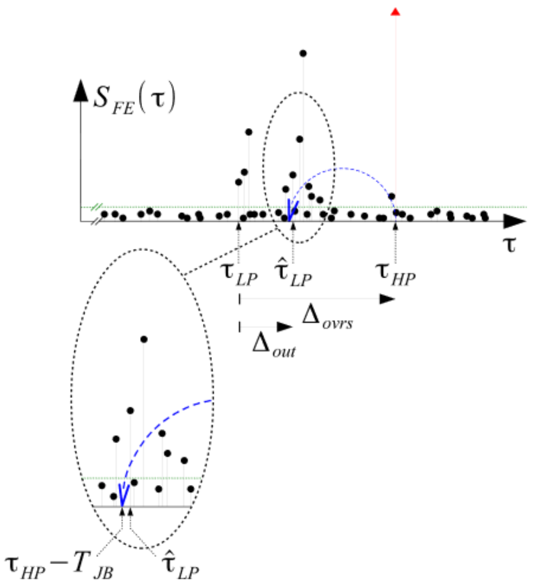
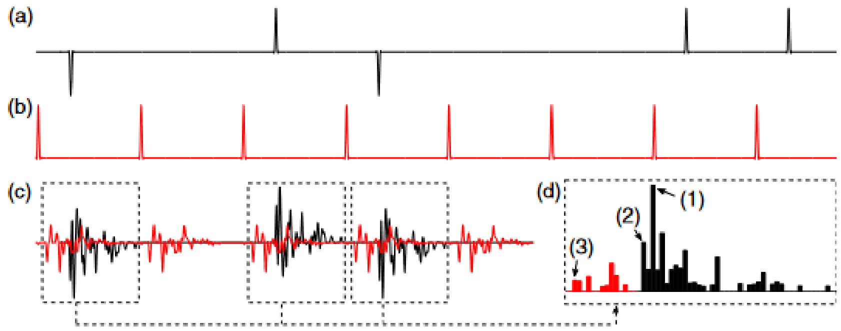


Figure 4.14: Overshadowing Attack, the red arrow indicates the attack peak. Image from [13]



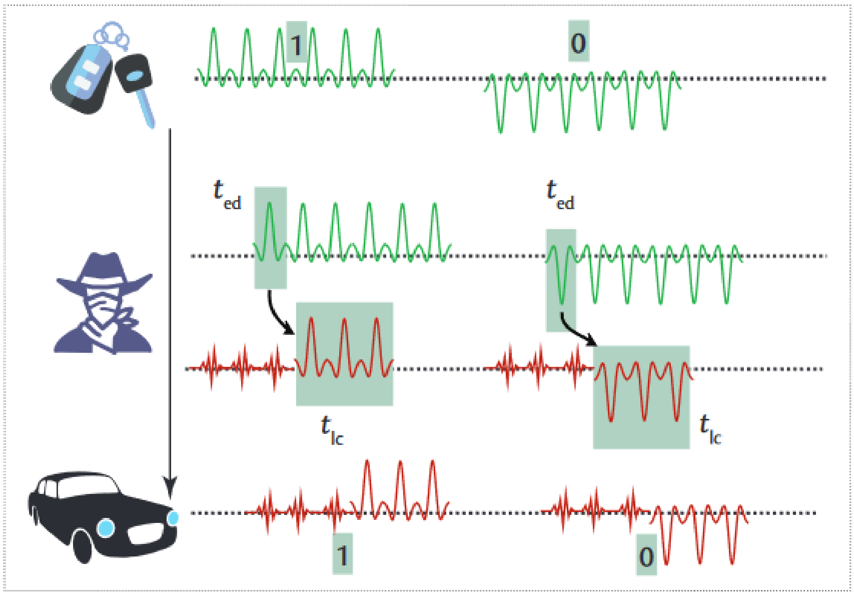
The cicada attack. (a) Benign transmitter T sends a preamble derived from a preamble code $[-1, 0, 1, -1, 0, 0, 1, 1, \ldots]$. (b) Attacker M transmits a cicada signal. (c) Both signals propagate through the multipath environment before they are received by R. (d) R aggregates the received signal over a number of pulses, and finds the strongest path (1). It then searches back for the first path (2), but instead finds the bogus path introduced by M (3).

Figure 4.15: Cicada Attack, Image from [38]

leading to a reduction in the distance when the leading edge algorithm estimates the ToF. The Cicada attack is shown in Figure 4.15.

In an Early Detect/Late Commit (ED/LC) attack, the attacker predicts the bit early even before receiving the entire symbol. Prior to this detection, the attacker can inject noise into the channel until the correct symbol can be predicted and committed. The attacker commits to this symbol later, leading to an increase in the measured distance [38]. This is shown in Figure 4.16.

All these attacks attempt to exploit the working of the leading edge algorithm or the predictable nature of the symbols. The IEEE standards committee took these issues into consideration and recently passed an amendment to improve the security. This amendment is known as the 802.15.4z for UWB HRP PHY. However, the standard document does not specify how to implement an algorithm to identify the time-of-flight in early path settings. It is left as a proprietary implementation detail to the manufacturers [47, 26].



Early-detect and late-commit attacks. An attacker can predict the bit (early detect; t_{ed}) even before completely receiving the symbol. The attacker then stops transmitting the arbitrary signal and switches, or "commits," to the bit corresponding to the predicted symbol (late commit; t_{lc}). Even though the received symbol contains an arbitrary signal at first, the car will correctly decode the symbol with the data that was committed late by the attacker.

Figure 4.16: Early Detect/ Late Commit Attack, Image from [39]

4.4. 802.15.4z Amendment

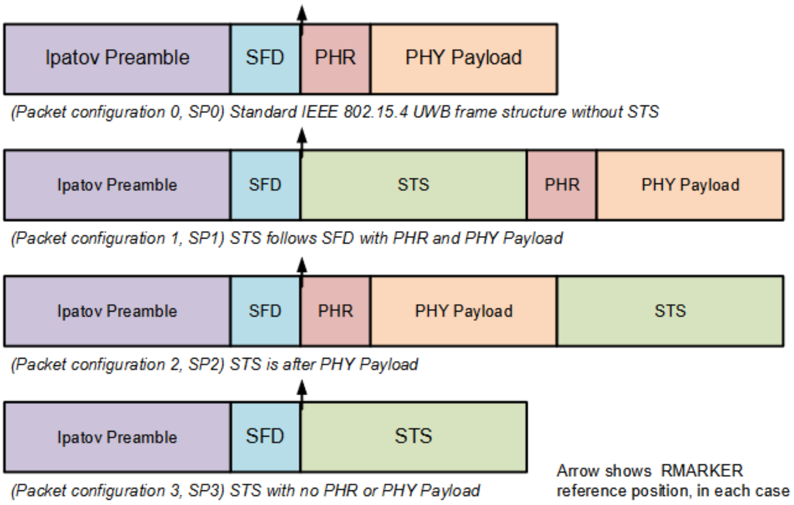

Ipatov Preamble
SFD
PHR
PHY Payload
(Packet configuration 0, SP0) Standard IEEE 802.15.4 UWB frame structure without STS
Ipatov Preamble
SFD
STS
PHR
PHY Payload
(Packet configuration 1, SP1) STS follows SFD with PHR and PHY Payload
Ipatov Preamble
SFD
PHR
PHY Payload
STS
(Packet configuration 2, SP2) STS is after PHY Payload
Ipatov Preamble
SFD
STS
(Packet configuration 3, SP3) STS with no PHR or PHY Payload
Arrow shows RMARKER reference position, in each case

Figure 4.17: UWB HRP PHY specified by the IEEE 802.15.4z amendment, Image from Decawave's DWM3000 User Manual [17]

The IEEE 802.15.4z amendment provides the HRP UWB PHY with means to address the above attacks, by introducing the Scrambled Timestamp Sequence (STS) field into the packet, as shown in Figure 4.17. The Ranging Marker (RMARKER) is used for the identification of the ToA from the received frame. The STS field consists of a set of pseudo-random Binary Phase Shift Keying (BPSK) modulated pulses, transmitted in one or more segments, which are each bounded by gaps i.e., time intervals during which the transmitter is silent. The pseudo-randomness of the BPSK modulation sequence is ensured by a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG), also referred to as Deterministic Random Bit Generator (DRBG), as recommended by the National Institute of Standards and Technology (NIST) [17]. The generation of the STS sequence is done by a 128 bit AES CSPRNG, as shown in Figure 4.18. Due to the pseudo-randomness of the sequence, there is no periodicity, allowing reliable, highly accurate, and artifact-free channel estimates to be produced by the receiver. For efficient decoding of the STS, the receiver needs to have a copy of the sequence locally available before the start of reception [27].

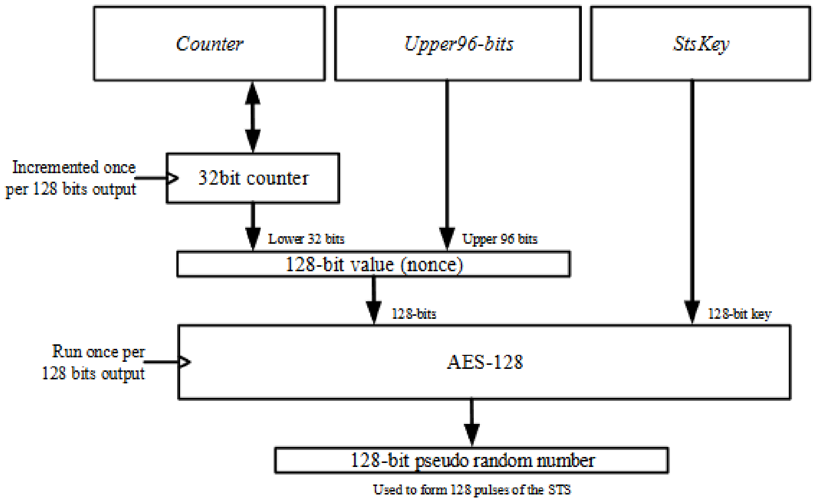

Counter
Upper96-bits
StsKey
Incremented once per 128 bits output
32bit counter
Lower 32 bits
Upper 96 bits
128-bit value (nonce)
128-bits
128-bit key
Run once per 128 bits output
AES-128
128-bit pseudo random number
Used to form 128 pulses of the STS

Figure 4.18: Key Generation for Scrambled Timestamp Sequence, Image from IEEE 802.15.4z standards [26]

4.4.1. Security of 802.15.4z

In [47], the authors present two new attacks, Cicada++ and Adaptive Injection Attack, that are possible in the newer standard. Both these attacks are based on the Cicada attack introduced by [38].

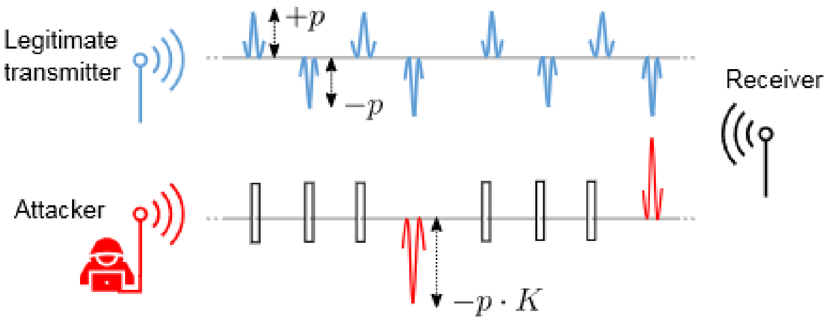


Figure 4.19: Cicada++ attack, Image from [47]
The adversary sends (random) pulses at a fraction of the PRF of the legitimate STS. The adversarial pulses are K times stronger.

In Cicada++, the attacker injects pulses at a fraction of the repetition frequency of the genuine transmitter. This leads to the energy of each attack pulse being stronger than the legitimate pulse. The adversary initially amplifies the legitimate signal to send it to the receiver in case the overall signal power is low. The attacker transmits its pulses in such a way that it synchronises with the legitimate

STS that is received by the receiver. They are presumed to possess knowledge of the received signal strength at the receiver, which lets them estimate the power to transmit the attack pulses [47]. This attack is shown in Figure 4.19.

In Adaptive Injection Attack, the attacker can control the granularity of the exact location of the injected peak. They are able to inject a peak exactly $\alpha \pm \epsilon$ ns earlier than the correlated peak in the CIR. α is the time advancement that the adversary wishes to achieve and ϵ is the inaccuracy. The attacker follows the same principles as in Cicada++. However in this case, after the attacker has relayed and injected a set number of pulses, they determine if they can succeed in injecting the peak at the intended position by correlating the legitimate STS pulses and the superimposed attack pulse-train. If the probabilities are in their favor, then they stop running their attack [47].

4.5. UWB Ranging

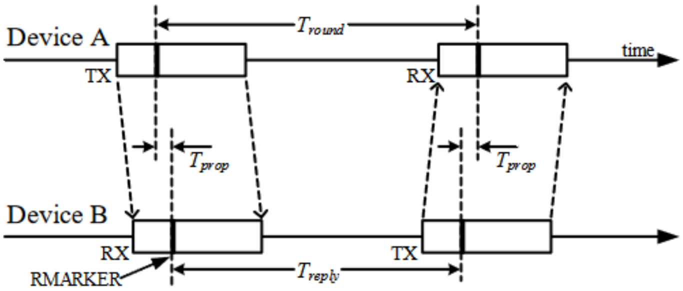


Figure 4.20: Single Sided Two-Way Ranging as specified by the IEEE standard, Image from IEEE standards on UWB [26]

In single sided two way ranging, there are two nodes. One acts as the initiator, beginning the range measurement, while the other node listens and responds to the initiator calculating the range. Single sided two-way ranging (SS-TWR) involves a simple measurement of the round trip delay of a single message from one node to another and a response sent back to the original node [26]. The operation of SS-TWR is shown in Figure 4.20, where device A initiates the exchange and device B responds to complete the exchange and each device precisely timestamps the transmission and reception times of the packets, and thus can calculate times T_{round} and T_{reply} by simple subtraction [17].

In summary, the latest standard introduces a timestamp sequence to prevent prediction of symbols, but the security parameters are not clearly defined. The leading edge detection algorithm to identify first path is not defined by the standard. Although the amendment attempts to address some attacks, it does not entirely solve all security concerns. There are two new proposed attacks that can lead to a reduction in the measured distance. This provides the basis of motivation for our proposed model, where we provide a solution to identify these anomalies.

5

CicadaSwat

In this chapter, we elaborate upon the system architecture of our proposed method, the threat model considered to evaluate its security, the working model of the proposed machine learning classifier, the environments considered to collect data, and the features processed from the gathered datasets to train the classifier.

A litany of research work in proximity detection methods exist that attempt to detect or measure proximity by focusing entirely on only one aspect of implementation. Contextual systems utilize a wide variety of radio signal information that is observed when the transmitter and the receiver exchange messages wirelessly, and use that for ensuring security when measuring distances. However, a mathematical upper limit on the distance between the two devices that can be provably ascertained is not possible on systems that utilize these methods.

Distance bounding based ranging techniques fit within this requirement, as they were specifically designed for measuring distances securely. However, they suffer from side-channel vulnerabilities due to being improperly realized. This is in part due to either their dependence on the underlying wireless signal protocol that is inherently insecure and unsuited for implementing distance bounding or due to latency issues such as processing delays that prevent the hardware that implements these algorithms from being accurate at measuring smaller distances. They are only accurate up to a few meters, which makes them unsuitable for critical solutions where security is paramount. Unfortunately, these techniques are completely oblivious of the contextual environment where they are used, which offer a lot of insight about the nature of the environment and radio signal characteristics.

The open-source algorithms proposed by the research community to account for the disparity in arrival time of signals especially in environments with a lot of delay spread, which is the time delay between the strongest signal and the earliest signal, do not consider any of contextual information that can be discerned from the received signals. Typical environments that exhibit high delay spreads include industrial and outdoor environments where NLoS conditions between the transmitter and receiver are prevalent. The cause of these delays may either be due to the presence of transient obstructions such as a person walking in between the two nodes or static obstructions such as concrete or wooden walls. The leading edge algorithm cannot differentiate between them and an adversary injecting signals that maliciously impact the Channel Impulse Response (CIR), and since the algorithm only takes into account the first path for ToA calculation, it makes the protocol vulnerable to exploitation by attackers. Motivated by these considerations and the absence of research work that to identify vulnerabilities in UWB HRP, we propose our model CicadaSwat.

5.1. System Architecture

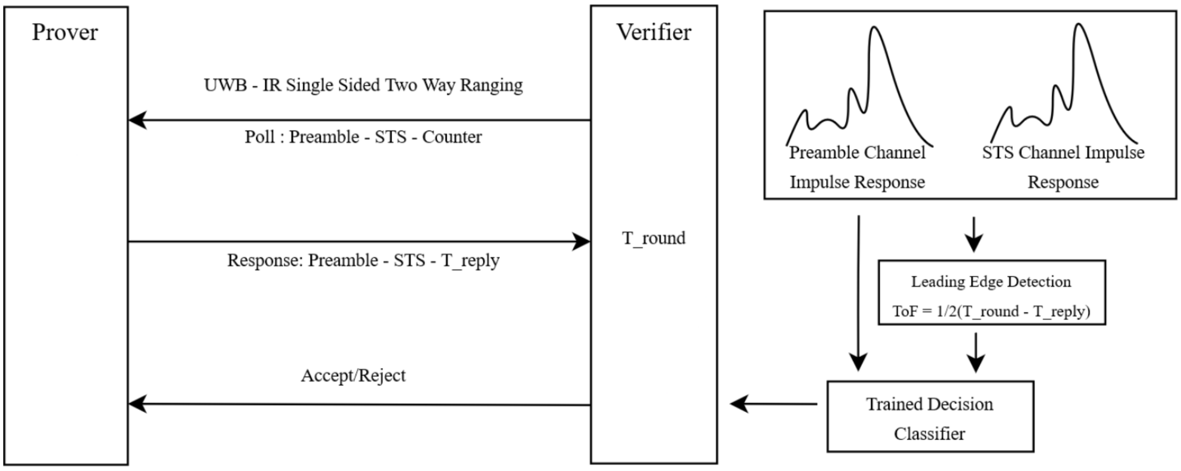

Prover
Verifier
UWB - IR Single Sided Two Way Ranging
Poll : Preamble - STS - Counter
T_round
Response: Preamble - STS - T_reply
Accept/Reject
Preamble Channel Impulse Response
STS Channel Impulse Response
Leading Edge Detection
ToF = 1/2(T_round - T_reply)
Trained Decision Classifier

Figure 5.1: System Model of CicadaSwat

In our proposed work, we utilize the CIR and several other features observed from radio signals, and compare them to previously observed values in that environment to bolster the security during subsequent measurements. CicadaSwat, shown in Figure 5.1, observes the CIR and signal characteristics from each ranging session. A ranging session is defined as the set of messages exchanged by the two nodes, transmitter/prover and receiver/verifier to complete one distance measurement.

In each ranging session, the verifier initiates the procedure by sending a poll message. The poll message consists of the preamble, the STS, and the lower 32 bits of the IV used for seeding the counter. The prover, upon receiving this frame, responds with a frame that contains the preamble, the STS generated by the next counter value, and the ToA of the poll frame as timestamped by the prover's leading edge algorithm. The verifier now estimates if the received STS is synchronised with the sequence it was expecting, by checking if the correlation between the locally generated STS template and the received STS is above a set threshold.

The verifier calculates the ToF using the embedded timestamp in the response message. If the measured distance matches the required threshold, it then extracts the CIR of the preamble and the STS from the received frame and measures similarity. Since both parts of the frame arrive one after the other in a short window of time and also take the same path to reach the antenna, they must exhibit similar characteristics [17]. This similarity in characteristics can be expressed by different parameters discerned from these two CIRs. For example, the ToF calculated using the preamble and the STS must be within a certain threshold of similarity. The measured channel power of the preamble and the STS must adhere to the FCC/ETSI standards, and the multi-path components as well as early path components observed in the both these CIRs must also be within set tolerances of similarity.

The verifier then calculates several different features from the CIR and other observations made from the received frame. A detailed overview of all features considered is provided in Section 5.4. The verifier then uses these features and sends them to the trained machine classifier which looks for anomalies in the observed data and then issues an accept/reject accordingly to complete the ranging session. For a clear understanding on how CicadaSwat detects attacks, we present the adversarial threat model in the following section.

5.2. System Adversary Model

In the case of NLoS conditions between the transmitter and the receiver, the highest correlation peak observed in the CIR may not necessarily be caused by the signal that arrived first. The received signals that the prover aggregates to measure the CIR may have been attenuated by several obstructions and/or undergone severe transformations leading to a drop in their transmission energies. Thus, the energy of the earliest component of the received signal may be attenuated, while the energy of the multipath components may not necessarily be as severely impacted due to them taking a different path. Since the receiver accounts for the earlier time of arrival using a leading edge algorithm, the attacker can exploit the algorithm to spuriously alter the distance by injecting signals that result in peaks observed.

5.2.1. Attacks by Adversary

For launching Cicada-TF, we assume that the adversary and the prover collude to circumvent the system i.e., the prover commits Terrorist Fraud, and the adversary is assumed to possess the knowledge of the STS sequence for that particular session. In Terrorist Fraud, the adversary's knowledge is only limited for one session, as the prover does not hand over any key material that lets the adversary launch future attacks independently. In this attack, the adversary and the prover are both outside the distance threshold range from the verifier, and they work together to reduce the distance measured by the receiver.

The attacker synchronises the transmission of their frame with that of the prover, but transmits the signals with a higher power than allowed by the regulations set by FCC/ETSI. These frames are received at the antenna of the verifier and the energies of all the individual pulses are aggregated. These aggregated pulses are then correlated with the locally stored template to calculate the CIR and identify the first path signal. However, due to interference caused by the presence of the malicious signal, the measured CIR contains spurious peaks inserted before the highest correlated peak and thus leads to the reduction in the measured distance. This attack works on the same principles as the Cicada attack, but the adversary is assumed to possess information about the STS for that particular session to overcome its unpredictability.

In Adaptive Injection attack, the adversary does not collude with anyone. The attack principles are the same as explained in Section 4.4.1. The attacker injects signals that are emitted with a fraction of the PRF of the transmitter thus leading to the larger energies of each individual malicious pulse being higher. The attacker stops transmitting their signal at the precise moment where the injected peak in the measured CIR leads to a reduction of required distance. The attacker can control this precision due to their knowledge of the CIR measured by the receiver. The fraction of the transmission chosen and We design our threat model around all these considerations.

We assume a strong attacker, who in addition to monitoring and injecting messages into the communication channels utilized using sophisticated hardware (Dolev-Yao model) [15], can also manipulate the channel contexts around the nodes i.e., manipulate environmental parameters such as the temperature, humidity, sound, and available radio information around the nodes. Moreover, the attacker can relay or block transmission of the genuine signals, and also possesses the knowledge of the CIR observed at the receiver. The attacker can also synchronise their transmission along with the transmitter, and their clocks. Finally, the attacker possesses an Additive White Gaussian Noise (AWGN) [9] channel to the receiver and can control the CIR observed at the receiver's antenna. In addition, the attacker also does not adhere to the FCC/ETSI limitations on the power of the transmitted signals. This threat model is similar to the one used by authors in [47].

5.3. Data collection

The classifier requires training data which it uses for identifying anomalies in the newer observations. The training dataset used must be exhaustive and capture as many different variations of ranging that may occur in an environment. In our work, the model is trained on labeled datasets. These datasets also contain points where attacks occur, such that the classifier is trained on both genuine and malicious runs. To prevent over-fitting of the classifier into one specific environment, the machine learning algorithm must be trained on multiple different environments. These environments must be diverse and must have different channel models. The IEEE 802.15.4a channel models report is used to identify suitable environments [34]. This report provides distribution models for the behaviour of UWB radio waves in different environments.

In this work we collect the datasets in three environments, namely an indoor environment, a closed outdoor environment and an office space. The performance of the model is evaluated against the two attacks in all three of these environments.

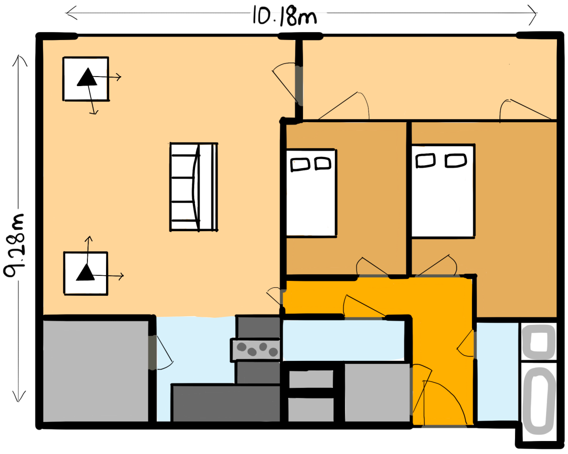


Figure 5.2: Environment 1, Indoor Residence

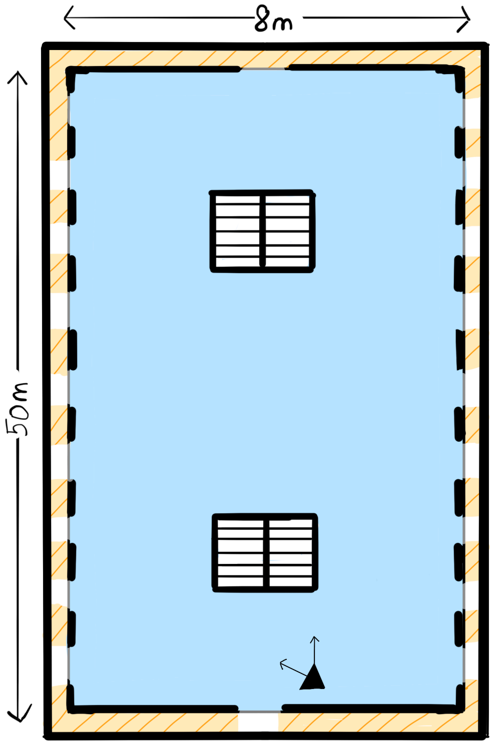


Figure 5.3: Environment 2, Outdoor passageway, Top View

Environment 1, shown in Figure 5.2, is an indoor residential area of 9.28m x 10.18m. The transmitter is placed at two locations in this environment, and the data was collected for each point from the system. Environment 2, shown in figures 5.3 and 5.4, is an outdoor passageway 50m x 8m. It has two sets of metal stairwells in the centre and has equally spaced doors on the left and right sides. Environment

3, shown in Figure 5.5, is an office space 14m x 8m wide. It contains several cubicles and tables separated from each other, and also concrete pillars on the right side. The numbered black triangle with the arrows in each of the images represent the positions of the transmitter and the direction of the antennae.

To gather an accurate fingerprint of the CIR within each environment, the data is collected at several points. These points are located in increments of 1m (in case of obstructions such as walls/furniture, they were placed at the closest possible location in increments of 50cm) from the transmitter. Reference measurements were made using a tape measure. In each of these points, the data is collected over the course of 15 minutes. The resultant dataset is pre-processed to remove any errors and spurious peaks. The total number of recorded observations is around is around 30,000. Additionally, to evaluate the efficacy of the model, different leading edge algorithms are used to compare performances, namely Search-Back and Jump-Back Search-Forward.

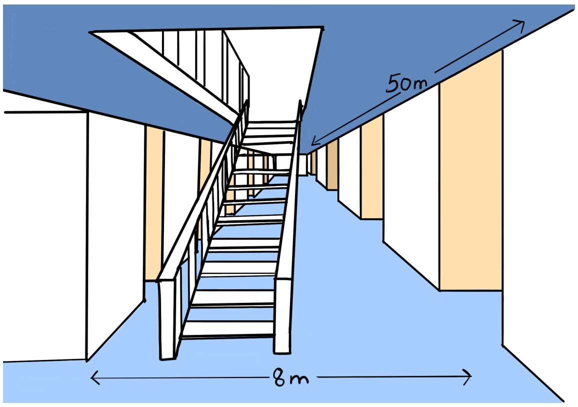


Figure 5.4: Environment 2,Outdoor passageway, Side View

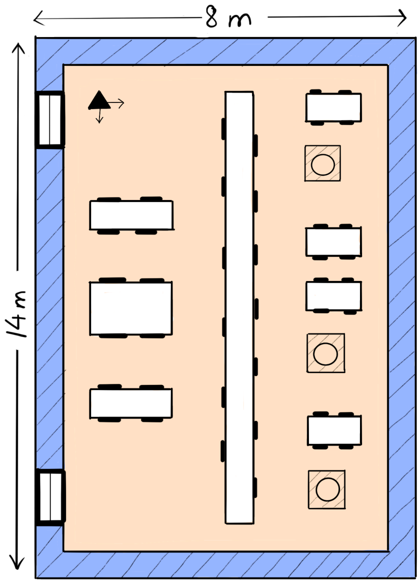


Figure 5.5: Environment 3, Office Space

The data collected during each ranging session contains the CIRs of the preamble and the STS. The location of the peaks and the first paths and also their powers as identified by the hardware, the clock offset between the two nodes, the ToA of the received signal identified by the leading edge algorithm and the measured distance. Information about the collected data and the features extracted is presented in the following section. Figures 5.6, 5.7, and 5.8 contain the fingerprints of the environments before pre-processing for all three leading edge algorithms.

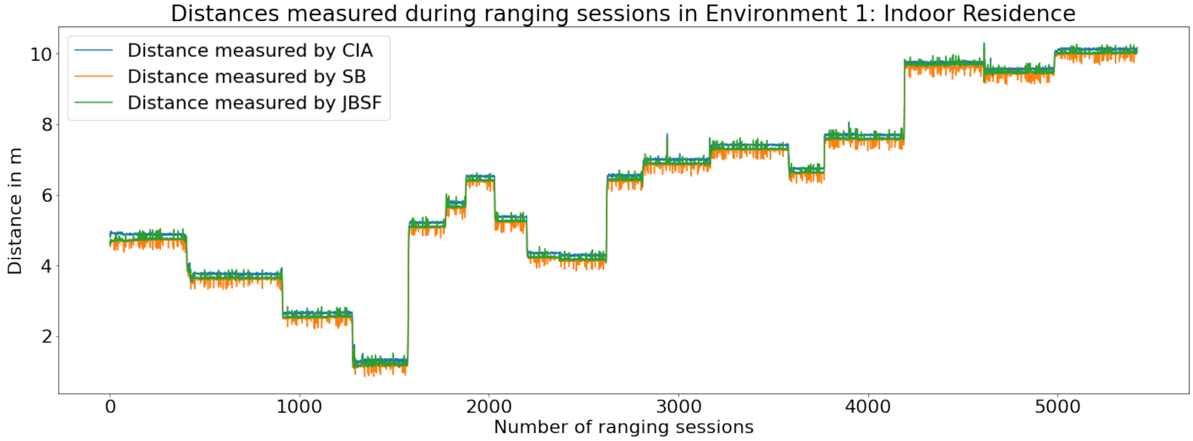


Figure 5.6: Fingerprint of entire environment 1 before pre-processing, for all three leading edge algorithms

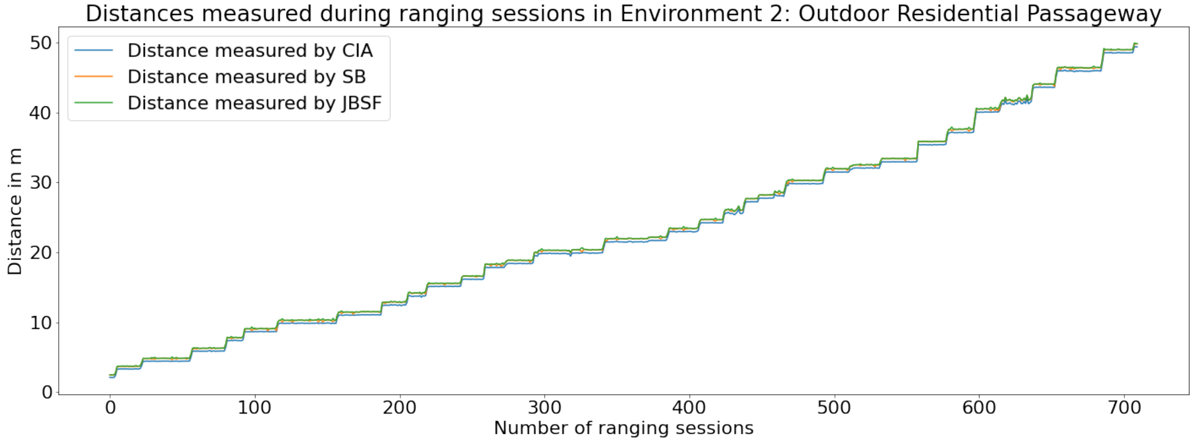


Figure 5.7: Fingerprint of entire environment 2 before pre-processing, for all three leading edge algorithms

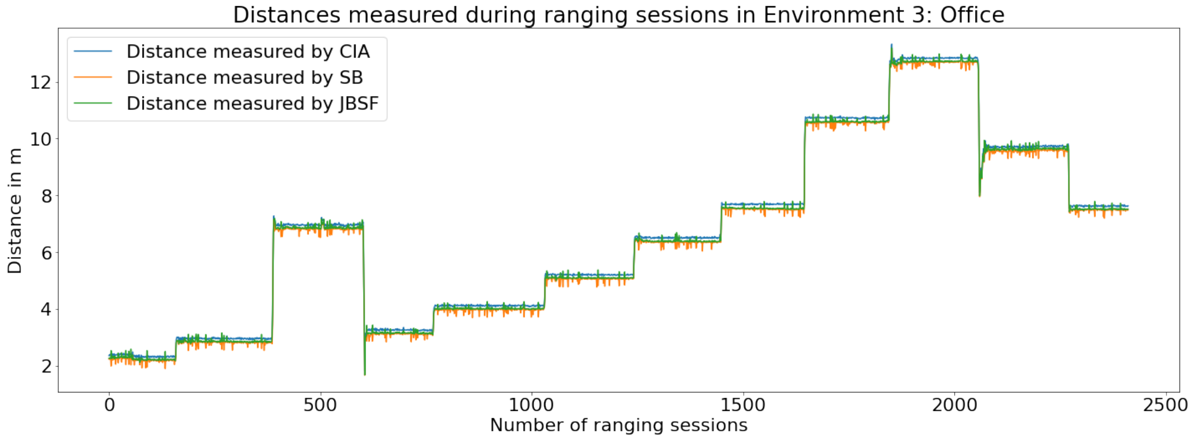


Figure 5.8: Fingerprint of entire environment 3 before pre-processing, for all three leading edge algorithms

5.4. Data Processing and Feature Extraction

In the latter stage of each single-sided two way ranging session, the verifier upon receiving the response sends the CIR of the received frame to the trained decision classifier, as shown in Figure 5.1. The CIR measured for both the preamble and the STS must be similar as they are both parts of the same frame, and take the same path to arrive. However, in the event of manipulation, it may be possible that there might be artefacts observed in the received signal wave. Therefore, the ToF calculated from both the preamble and the STS must be similar within a certain threshold. The CIR can also be used to identify the presence of a clear LoS between the transmitter and the receiver, and other channel conditions such as the environment noise, multi-path components, and presence of early path signals. Feature selection for the collected data was done based on extant literature that use machine learning techniques to identify anomalies in observed radio signals as in [54, 29] and preliminary experiments performed that offered insight into the different parameters that affect ranging sessions.

The following features were selected and calculated from the observed CIR:

- **Noise Threshold**: The measured signal noise in the channel that is observed. In environments with a lot of noise, the leading algorithm may incorrectly identify first path from the noise peaks and a a high threshold results in first path components being ignored.The noise threshold is identified per ranging session and it is the root mean squared value of the magnitudes in the initial parts of the CIR. This was calculated as described by the [17]. An attacker may inject noise into the channel in an attempt to make the leading edge algorithm choose a spurious peak and reduce distance, thus it is a pertinent feature considered.
- **Power of the Peak**: The measured power at the highest correlated peak in the CIR. An adversary not adhering to FCC/ETSI regulations may amplify the power of transmitted signals, and high values of power at large distances may indicate the presence of attacks. Additionally, the loss in energy of radio signals as they propagate in free space must be commensurate with the measured distance. The power also provides an insight into the observed power due to attenuation or obstructions.
- **Power of First Path Signal**: The measured power of the identified first path of the signal. The first path power can be used to gather insight about several things. For example, if the powers of the peak and first path component are similar then it may indicate that the transmitter and the receiver have a clear LoS. A very low first path power indicates that the energy was attenuated heavily which may be due to several obstacles present between the two nodes, whereas a slightly lower energy than the peak indicates the presence of simpler obstacles like walls.
- **Signal to Noise Ratio** : The ratio of the overall power of the received signal to the level of background noise. SNR is expressed in decibels (dB). This ratio offers insight into the overall signal quality of the received frame, a high value indicates the presence of low noise and a clear distinction of the observed radio signal while a lower values signifies a drop in quality.

$$SNR_{dB} = 10log_{10}(P_{Signal}/P_{Noise}) \tag{5.1}$$

P_{Signal} - Power of signal

P_{Noise} - Power of Noise

- **Clock Offset**: The offset between the clocks of the transmitter and the receiver. Measured in parts per million as described in the IEEE standard. The clock offset is generated by the hardware during reception of each packet as the receiver locks on and compensates for the frequency offset of the transmitting device to successfully receive a packet. An attacker launching Adaptive Injection attack would have to first synchronise with the receiver and then detect the original transmission which is followed by amplifying it. The underlying radio signal undergoes several transformations and since each hardware has imperfections due to which the exact carrier frequency of the crystal oscillator is slightly different, the subsequently generated signal incorporates all these features [29].
- **First Path to Peak Delta**: The distance between the peak and the first path observed in the frame (in number of samples). This provides an indication into the delay spread observed in the ranging session. Several insights can be discerned from this feature. A very low value indicates that the identified first path and the peak are located close to each other which is a strong indication for LoS, an extremely high value may indicate a possible occurrence of an attack if the observed value does not correlate with the rest of the chosen features.
- **Kurtosis**: The kurtosis of the CIR. The kurtosis is a measure of the “peakedness” of the sampled signal in the time domain [29]. The propagated signal that reaches the receiver may contain several multipath components, in addition to being impacted by the noise present in the channel.

The kurtosis of the CIR offers insight into the type and distribution of peaks that are present in the dataset. A negative kurtosis value indicates that the CIR has several peaks that are similar in magnitude, which may be used as a strong indication of an NLoS scenario where as a positive value indicates LoS and a clear correlation peak observed from CIR. The kurtosis is defined as the fourth standardized moment of a distribution, used for describing its shape.

$$Kurt[x] = \frac{\mu_4}{\sigma^4} \tag{5.2}$$

μ - Fourth central moment

σ - Standard Deviation

5.4.1. Model Training

The generated datasets along with their features are used for training the machine learning classifiers. For the detection of anomalies during ranging, we evaluate three classifiers: Logistic Regression, Random Forest and K-Nearest Neighbours. These classifiers were chosen based on extant literature that exhibit high accuracies when utilizing them [54, 29] The machine learning classifier is trained using 10-fold nested cross-validation as the number of samples with successful attacks is low i.e., there is a class imbalance caused by the dataset containing larger number of genuine ranging sessions than attacks. The following hyperparameters are chosen to evaluate the classifiers:

- **Logistic Regression:** C: [1,5,10], solver : [newton-cg, lbfgs, liblinear]
- **Random Forest:** n estimators: [5,10, 50, 100, 200], max depth: [5,10,15,50], criterion: [gini, entropy]
- **K-Nearest Neighbours:** n neighbors:[5,10,15,20], algorithm: [ball tree, kd tree]

The hyperparameters are tuned using gridsearch on all the considered classifiers. Details about the experimental setup, the hardware used and results of evaluation of our proposed model are described in Chapter 6.

6
Experimental Setup and Result Evaluation

In this chapter, we provide a description of our experimental setup, preliminary experiments and their results, which act as the basis for data collection conducted in three separate environments selected. Finally, we present the results of performance evaluation of CicadaSwat.

For the implementation and experimental verification of our proposed model, the items described in Table 6.1 are used. The DWM3000 Integrated Circuit (IC), manufactured by Decawave, is a 802.15.4z certified UWB chip. It is the newer variant released recently as an upgrade over their DWM1000 IC, which supported only the 802.15.4a protocol.

Hardware/Software	Manufacturer
DWM3000	Decawave
NRF52840-DK	Nordic Semiconductors
C API SDK for DWM3000, NRF52840-DK	Decawave, Nordic Semiconductors
Scikit learn	Python

Table 6.1: Hardware and Software used for the experimental setup

DWM3000, as shown in figures 6.1 and 6.2, is designed to be compliant to the FiRa PHY and MAC specifications enabling interoperability with other FiRa compliant devices, it is further interoperable with the Apple U1 chip. The current Pixel 6 devices incorporate this chip for their UWB requirements. The DWM3000 module is compatible with the BPRF mode in UWB HRP PHY, and supports a PRF of 64 MHz. Currently, these ICs are being shipped as engineering samples and have not entered widespread manufacturing yet.

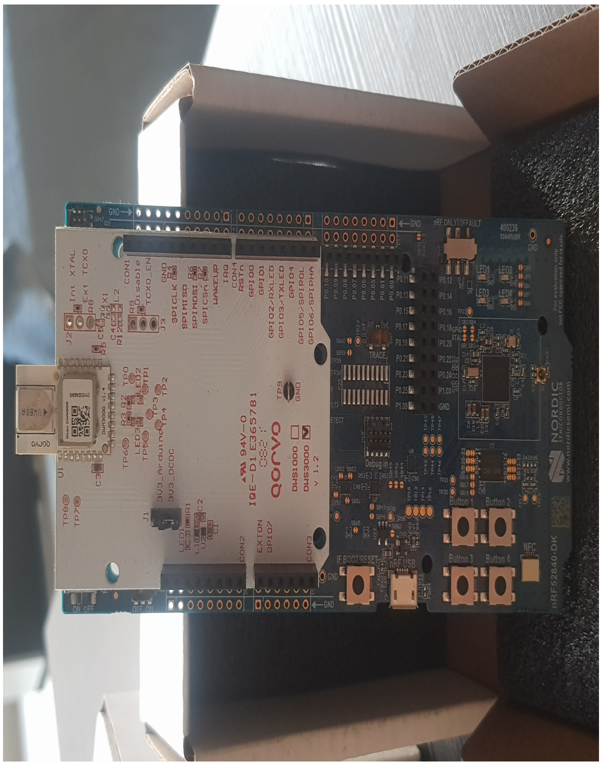


Figure 6.1: DWM3000 UWB IC (White) mounted on NRF52840-DK (Blue) by Decawave

The NRF52840-DK, as shown in figures 6.1 and 6.2, is a versatile single board development kit for Bluetooth Low Energy, Zigbee, 802.15.4 and other 2.4 GHz applications on the nRF52840 SoC. It is Arduino Uno Revision 3 compatible, making it possible to mount 3rd-party shields with ease. The DWM3000 shield interfaces with the NRF52840 which connects to a PC using USB. The API SDKs (Software Development Kit) used are provided by the individual manufacturers of the chip i.e., DWM3000 API SDK is provided by Decawave, whereas NRF52840 API SDK is provided by Nordic Semiconductors. The DWM3000 API SDK builds upon the NRF API SDK and is used to drive the IC. These APIs are used to program the ICs as receivers/transmitters.

We use three such chips for all experiments performed, as shown in Figures 6.3, with two nodes being used as the receiver and transmitter, and the third node being used to mount attacks on the

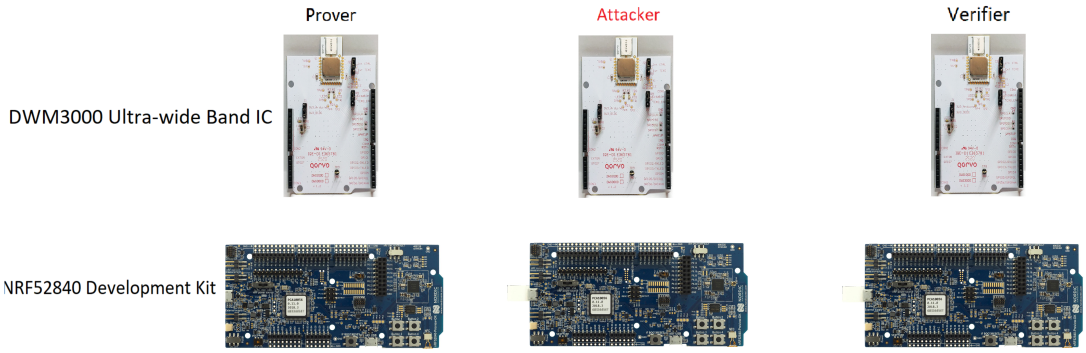


Figure 6.2: Hardware used for CicadaSwat

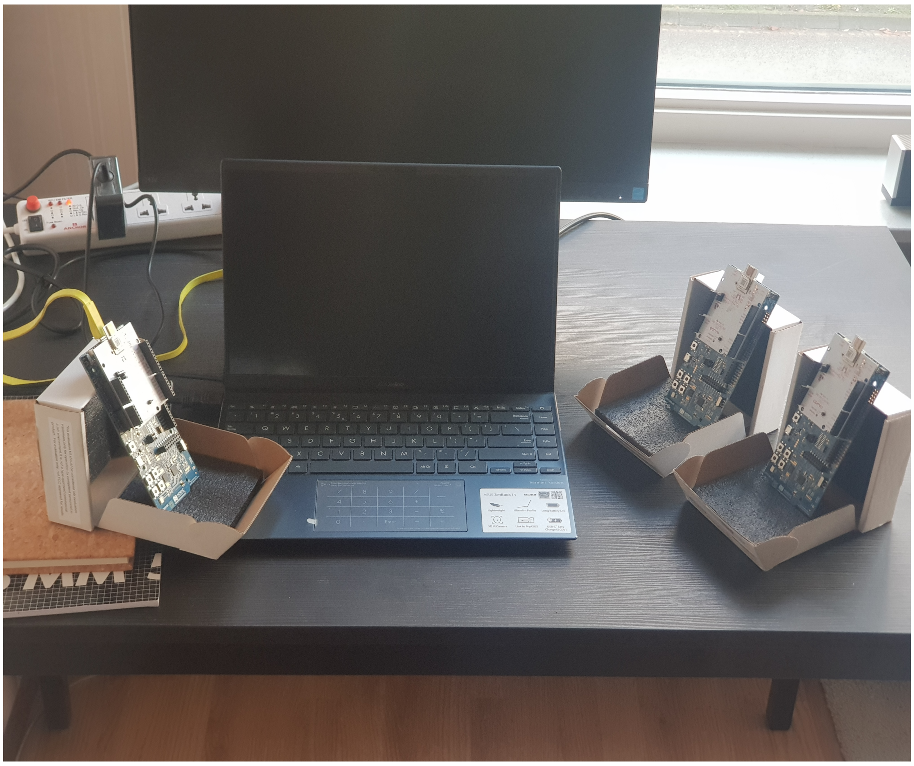


Figure 6.3: Experimental Setup of CicadaSwat

system. For each ranging session, the DWM3000 writes metadata to the serial port. The PC is used to monitor the serial output which is then written to a file and stored in a JSON (Javascript Object Notation) format. The metadata output by DWM3000 includes the measured distance, power levels of the signal, the contents of the diagnostics register, and the CIR of the preamble and the STS (as mentioned in the user manual [17]). This experimental setup is shown in Figure 6.2.

The CIR measured by the DWM3000 chips is an estimate of the observed channel [17]. The measured channel power and the first path power of each frame at the end of an ranging session are also both estimates, and vary slightly from the actual values. These values are estimated by using the measurements from the DWM3000 hardware and the specifications outlined by the user manual [17].

6.1. Preliminary Experiments and Results

To characterise LoS and NLoS scenarios and study the effect of different obstacles, multiple experiments were performed. Different obstructions were used during ranging to model the NLoS scenarios such as open/closed doors, concrete walls/wooden walls, people walking, and the difference in CIRs

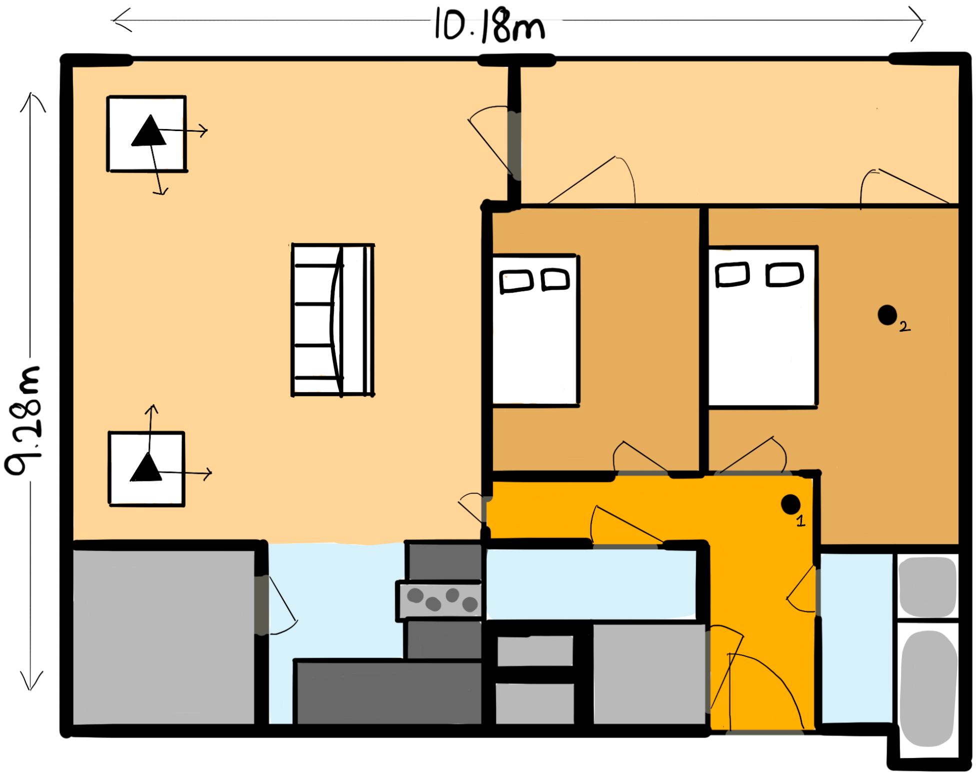


Figure 6.4: Environment 1, Indoor Residence

is observed. In Figure 6.5, the experiment was performed at $5m$ with LoS, and then at $7.8m$ (point 1 on Figure 6.4) with LoS and NLoS which was induced by opening and closing the door. There is a noticeable yet small spike in the measured distance between the two nodes when the door was closed. The individual transient spikes observed are caused due to people crossing the ranging session. The measured distances here are reported from the manufacturer's proprietary leading edge algorithm, Channel Impulse Analyzer (CIA) [17].

While there is a noticeable peak in the measured distance when the door was closed and opened, the actual increase in distances is well within the tolerances of error of the measured distance $(10 - 20cm)$. The tolerance of error is used for accuracy of the hardware, DWM3000 is accurate upto $10cm$. The impact on the Channel Impulse Response is also negligible. This is shown in figures 6.6 and 6.7. In Figure 6.6, the measured distance is $7.87m$, and in Figure 6.7 the measured distance is $8.02m$. The real distance was $7.80m$.

When the same experiment is repeated at Point 2, shown in Figure 6.4, inside the room the observed CIR is much different. This can be observed in the Figure 6.8, where a clear first-path component is introduced into the signal. This is due to the signal passing through the several walls and getting attenuated.

The two leading edge detection algorithms, jump-back-search-forward and search-back, are implemented for identification of ToF. The distances measured by all three algorithms for the entire fingerprint, before pre-processing for Environment 1 is shown in Figure 5.6. The tolerances of error for all three algorithms are within the set threshold of $1.5m$. This threshold is the same as chosen by authors in [47]. The CIA leading edge algorithm has the lowest error as observed from the graphs.

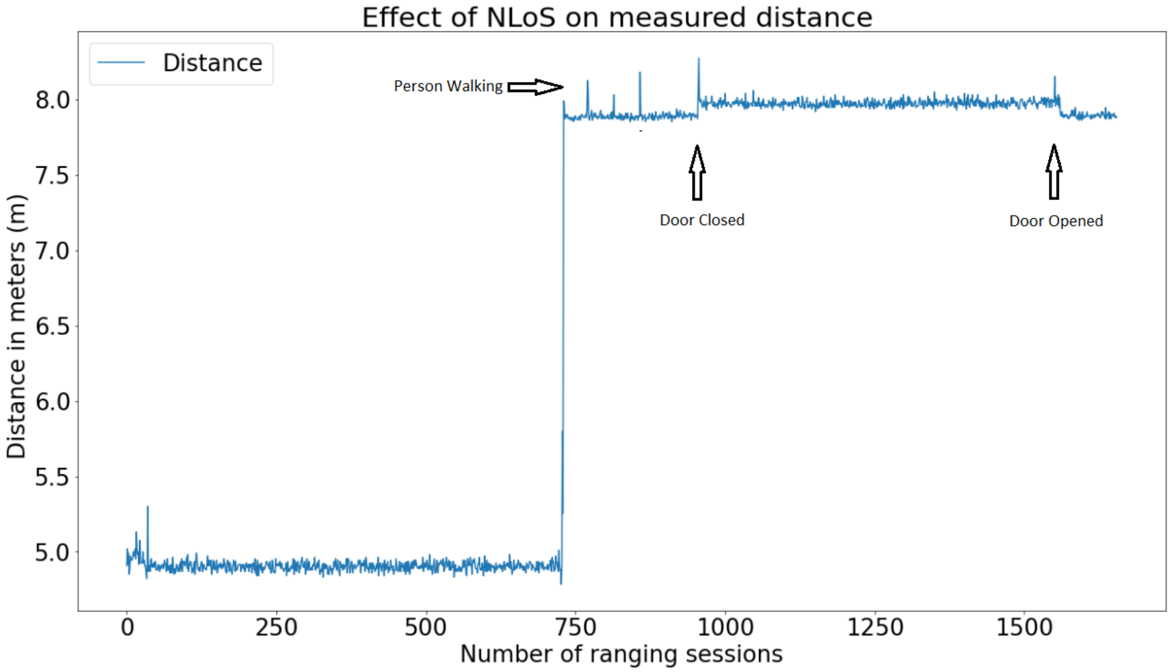


Figure 6.5: Experiment to measure impact on NLoS due to obstacles

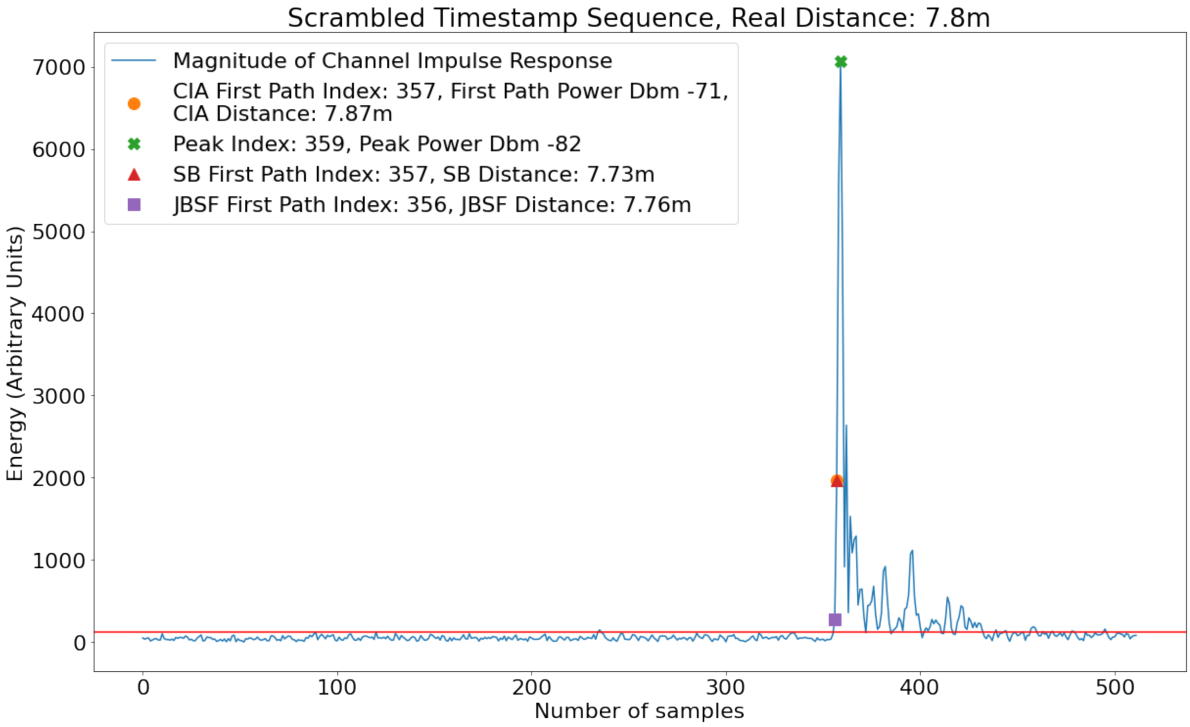


Figure 6.6: Impact on NLoS Point 1 Scenario 1: Door Open

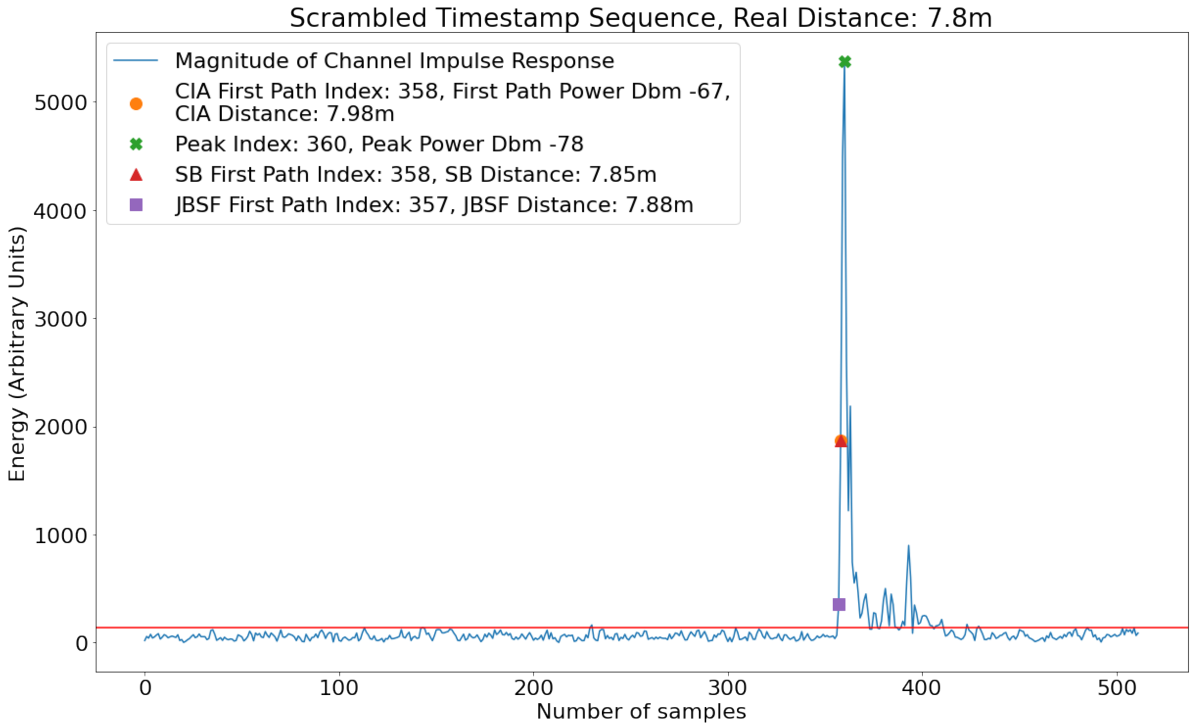


Figure 6.7: Impact on NLoS Point 1 Scenario 2: Door Closed

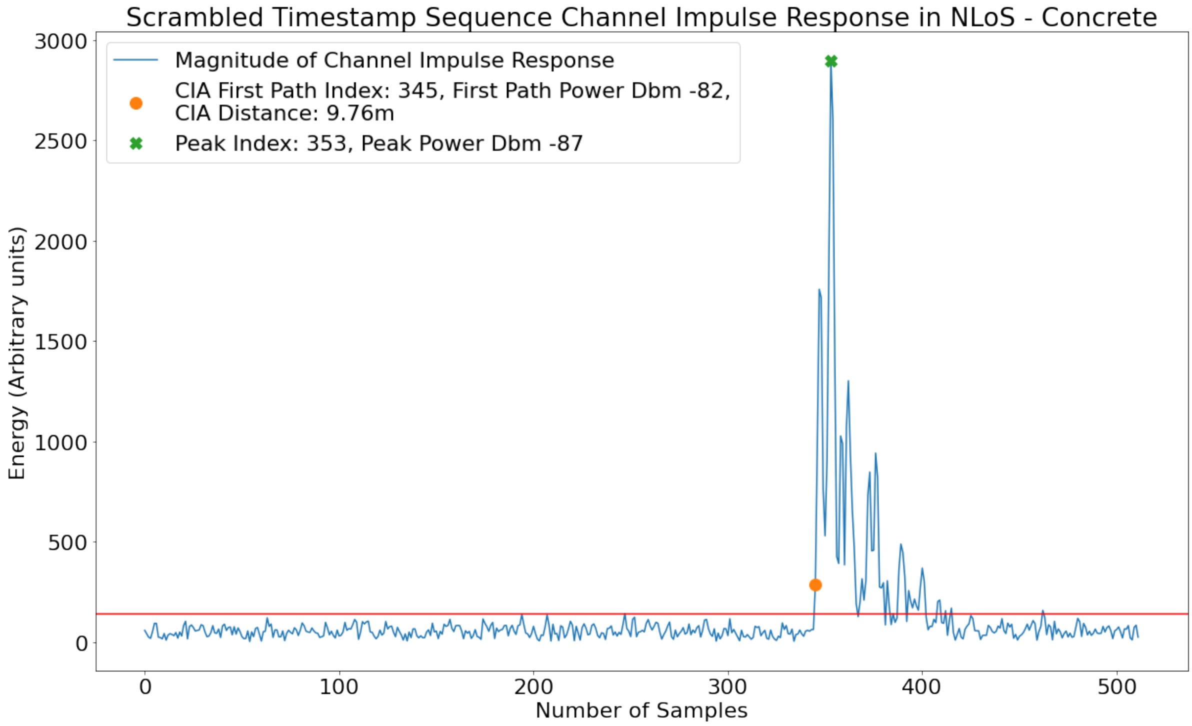


Figure 6.8: Impact on NLoS at Point 2

6.2. Mounting Attacks

6.2.1. Cicada-TF

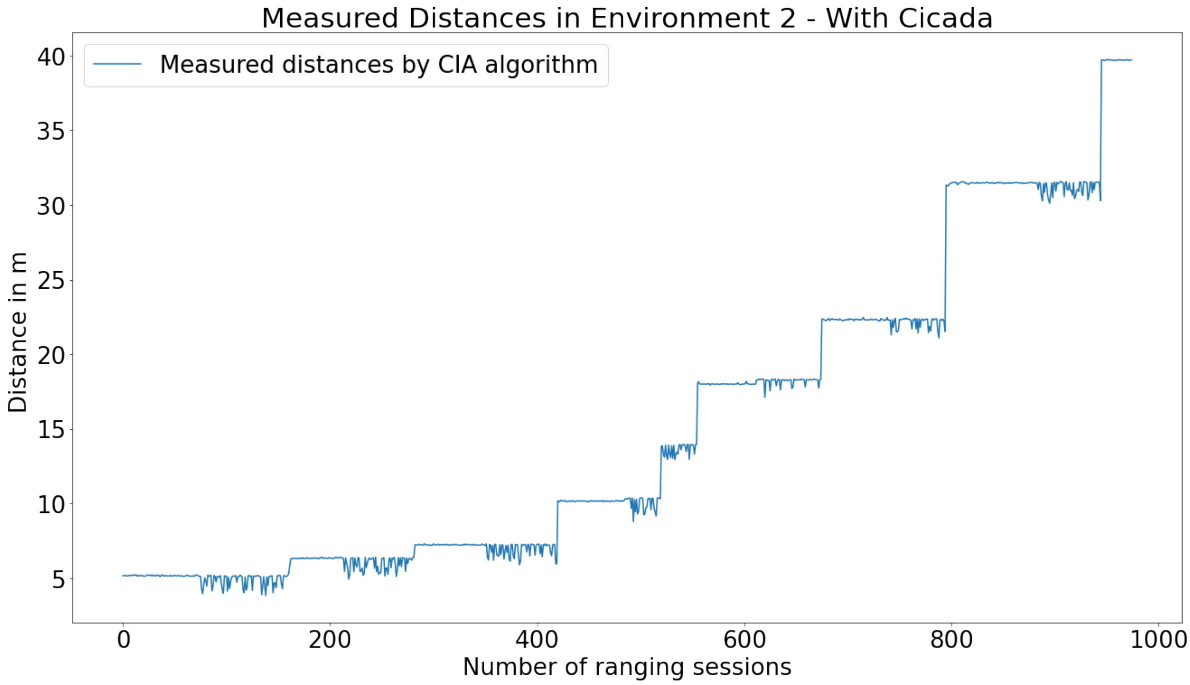


Figure 6.9: Cicada Attack in Environment 2, Each point consists of 15 minutes of normal ranging and 15 minutes of attacks

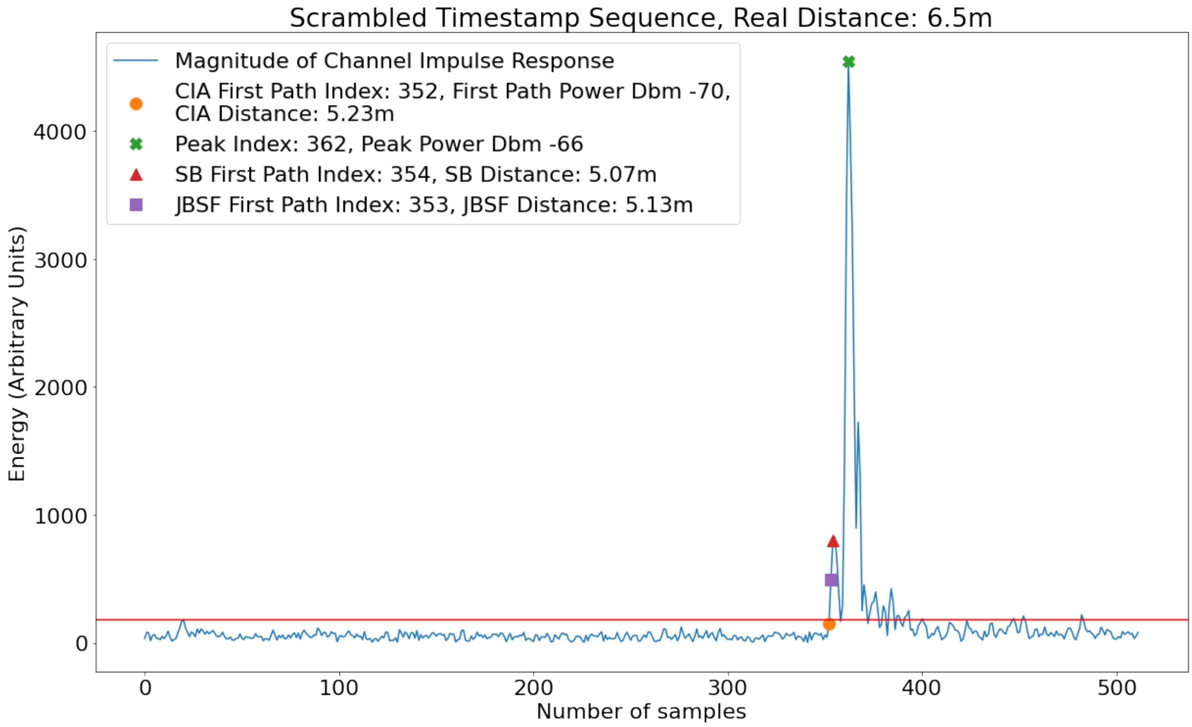


Figure 6.10: Cicada Attack in Environment 2, Channel Impulse Response

For mounting the Cicada-TF attack, the prover and the adversary DWM3000 ICs are synchronised to each other using a jumper wire connecting two general purpose input/output pins. The Cicada-TF attack requires that the adversary chirps with signals alongside the genuine transmissions. This leads to an early path component introduced when the receiver measures the aggregated energy received at its antenna. In Cicada++, the adversary's PRF (chirp rate) is a fraction of the actual PRF of the genuine signal. Since the DWM3000 chip does not support a 16 MHz PRF (1/4th of 64 MHz PRF in BPRF) when transmitting the STS, the number of ranging sessions in which a spurious first-path signal is introduced is reduced. However, this attack can still be observed quite clearly. The adversary also transmits signals with a higher power than the genuine transmitter and this was controlled using the registers provided by DWM3000 for this purpose [17]. In Figure 6.9, the environment consists of datapoints where 15 minutes of normal ranging sessions and 15 minutes of ranging sessions where Cicada-TF was launched is shown. Figure 6.10 contains the equivalent channel impulse response for a session where an attack has occured. The real distance is 7.1 meters, but the measured distance by the leading edge algorithms is around 6m each.

6.2.2. Adaptive Injection Attacks

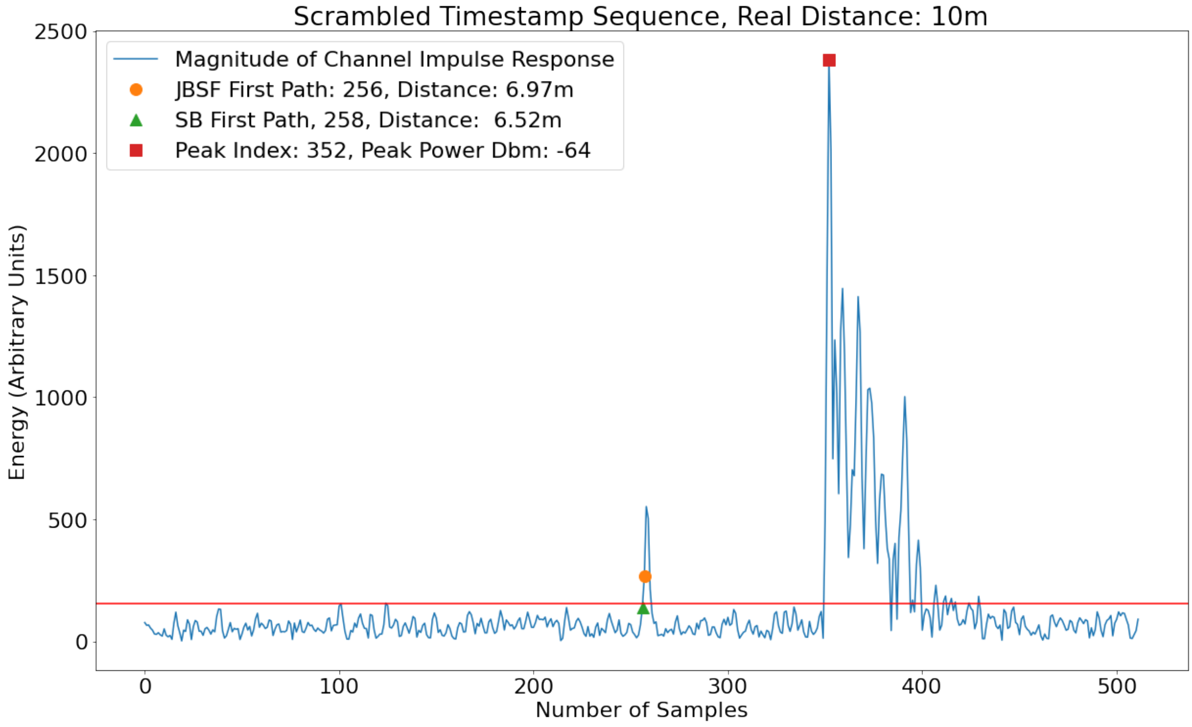


Figure 6.11: Effect of Adaptive Injection Attack on Channel Impulse Response

In this attack, the adversary uses a similar setup as in Cicada++, but the adversary has a higher advantage and can precisely control where the spurious first path peak is to be injected. This is a much stronger attack, as the adversary can control the reduction in distance that is desired. Furthermore, no knowledge about the STS is required. The attacker possesses knowledge about the received CIR power by the verifier, and can directly control what they receive. This attack requires also requires an adversary to chirp at a fraction of the total rate. To overcome this requirement, the attack is simulated by directly injecting spurious peaks at the required sample location of the CIR. This location is chosen from the parameters with the highest success rate as shown in [47]. The injection of a peak indicates an attack has succeeded and when the prover utilizes the inbuilt leading edge algorithm to measure the distance, they incorrectly identify the malicious peak as the first path edge. The CIA algorithm cannot be utilized in this case, as the IC automatically runs the algorithm when a ranging frame is received and cannot be manually triggered. Evaluation for this attack is performed for only for the other two leading edge algorithms. An example of a successful Adaptive injection attack is shown in Figure 6.11.

6.3. Results

In this section we report the results achieved by CicadaSwat in the three environments against both the attacks, Cicada-TF and Adaptive Injection Attack.

LDE/Classifier	Random Forest	Logistic Regression	K Nearest Neighbours
Channel Impulse Analyzer (CIA)	95.3%	75.5%	81.5%
Jump-Back Search-Forward (JBSF)	94.1%	74.7%	79.3%
Search-Back (SB)	94.1%	74.4%	79.80%

Table 6.2: Results of evaluation of CicadaSwat against Cicada-TF in Environment 1

LDE/Classifier	Random Forest	Logistic Regression	K Nearest Neighbours
Channel Impulse Analyzer (CIA)	98.8%	97.2%	94.39%
Jump-Back Search-Forward (JBSF)	97.39%	90.2%	91.2%
Search-Back (SB)	96.0%	90.10%	89.1%

Table 6.3: Results of evaluation of CicadaSwat against Cicada-TF in Environment 2

LDE/Classifier	Random Forest	Logistic Regression	K Nearest Neighbours
Channel Impulse Analyzer (CIA)	99.3%	97.1%	98.2%
Jump-Back Search-Forward (JBSF)	97.39%	97.1%	94.6%
Search-Back (SB)	96.8%	92.0%	93.89%

Table 6.4: Results of evaluation of CicadaSwat against Cicada-TF in Environment 3

6.3.1. Cicada-TF

For the Cicada-TF attack, as shown in tables 6.2, 6.3 and 6.4, it can be discerned that the best classifier was observed to be Random Forest and the leading edge algorithm with the highest accuracy was Decawave's Channel Impulse Analyzer (CIA) algorithm. This is not surprising as the CIA applies several statistical tests before choosing the first path [17] and overall exhibited the highest accuracy. The CIA takes multiple contexts gathered during ranging into consideration, performs statistical tests that these contexts must adhere to before it allows for successful ranging. In Cicada-TF, the attacker does not exercise clear control on the positions of the injected peaks. Unsurprisingly, the Search-Back algorithm lead to the largest drops in accuracy in all observed classifiers. This is because of the nature of its working, where a large noise only section must be observed before the first path signal is identified. This use of the large back-search time window makes it susceptible to choosing spurious peaks as the first path, as an attacker could inject signals into the channel that prevent this algorithm from reaching a noise only region. Logistic Regression was the worst-performing classifier in all three environments, especially when utilizing the Search-Back algorithm.

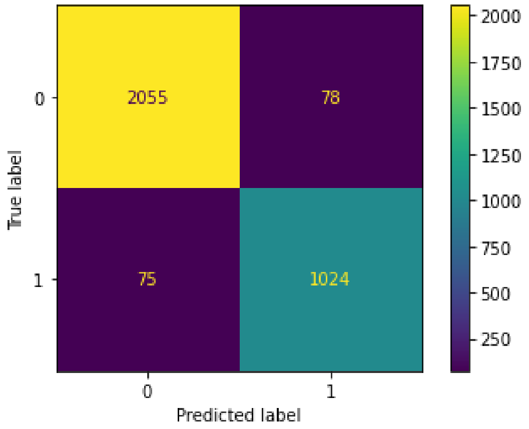


Figure 6.12: Environment 1, Random Forest Criterion: Gini, Max Depth:50

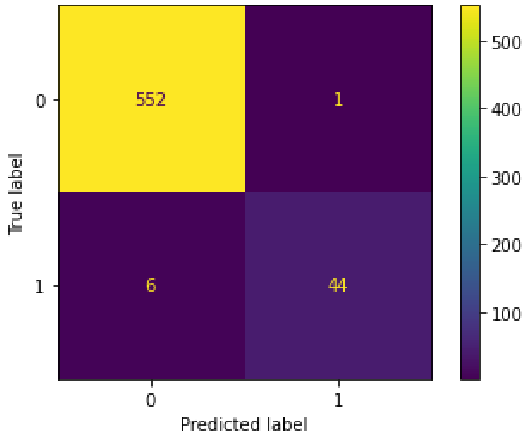


Figure 6.13: Environment 2, Random Forest Criterion: Gini, Max Depth:15

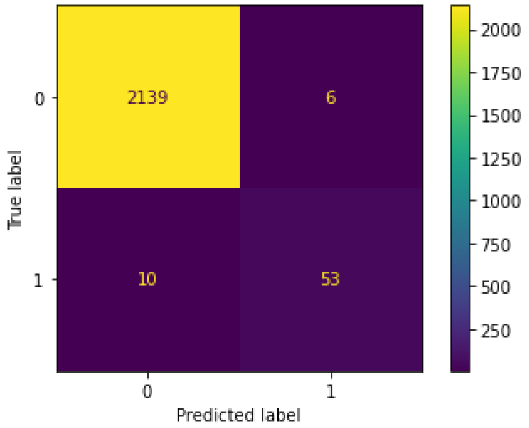


Figure 6.14: Environment 3, Random Forest Criterion: Entropy, Max Depth:50, N Estimators: 50

Figure 6.15: Best model selected for Cicada-TF Attack

6.3.2. Adaptive Injection Attacks

The performance can be observed to be similar to that of Cicada-TF. The model with the best performance in this case was also Random Forest, albeit marginally. The overall accuracies of the model in this attack were relatively lower, this may be attributed to the cause that the attacker is able to very

LDE/Classifier	Random Forest	Logistic Regression	K Nearest Neighbours
Jump-Back Search-Forward (JBSF)	94.1%	71.6%	79.1%
Search-Back (SB)	88.4%	70.23%	78.6%

Table 6.5: Results of evaluation of CicadaSwat against Adaptive Injection Attack in Environment 1

LDE/Classifier	Random Forest	Logistic Regression	K Nearest Neighbours
Jump-Back Search-Forward (JBSF)	94.6%	89.2%	90.3%
Search-Back (SB)	92.39%	88.7%	89.8%

Table 6.6: Results of evaluation of CicadaSwat against Adaptive Injection Attack in Environment 2

LDE/Classifier	Random Forest	Logistic Regression	K Nearest Neighbours
Jump-Back Search-Forward (JBSF)	91.24%	90.7%	88.79%
Search-Back (SB)	90.35%	88.4%	87.3%

Table 6.7: Results of evaluation of CicadaSwat against Adaptive Injection Attack in Environment 3

precisely control the nature and power of the peak that is injected. It can be discerned from the results that utilizing statistical features to identify the presence of attacks is highly probable. The proposed model exhibits robust accuracies in varied environments. More research work is required in this direction, to confirm the efficacy of our model in environments with more NLoS conditions and channel delay spreads. The drop in accuracies by the classifiers in the case of Adaptive Injection Attacks can be attributed to the location and amplitude of the injected peaks.

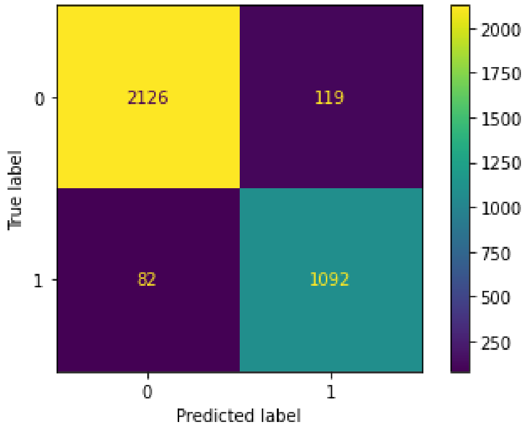


Figure 6.16: Environment 1, Random Forest Criterion: Gini, Max Depth:15, N Estimator: 200

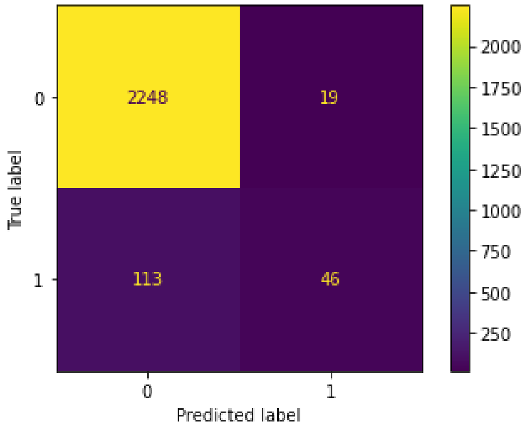


Figure 6.17: Environment 2, Random Forest Criterion: Gini, Max Depth:15

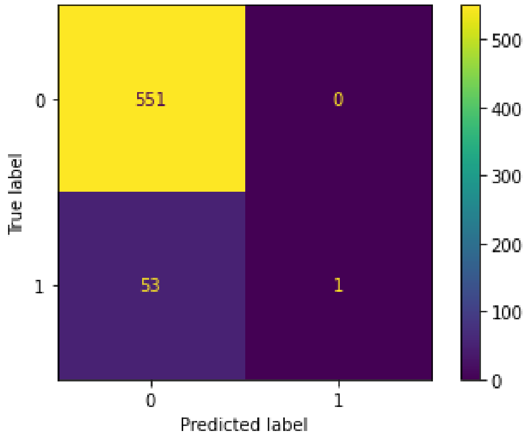


Figure 6.18: Environment 3, Random Forest Criterion: Entropy, Max Depth:50

Figure 6.19: Best model selected for Cicada-TF Attack

Environment 1 exhibited considerably lower accuracies with both logistic regression and k nearest neighbours when compared to random forest. This can be attributed to the presence of several NLoS locations with small passageways, walls, and other obstructions within environment 1. Furthermore, environment 1 contains more locations with higher delay spreads than observed in other environments. Environments 2 and 3 are have more points with a clear LoS between the prover and the verifier due to which the accuracies are higher. The confusion matrices for the best models are shown in figures 6.15 and 6.19.

The best features reported by the Random Forest classifier were found to be the first path to peak delta, the first path to peak ratio, kurtosis and the measured distance. These features correlated highly with the occurrence of attacks in the three environments. More work is needed in this direction to verify the applicability of these features in other environments.

7 Conclusion and Future Work

7.1. Conclusion

In this report, we proposed CicadaSwat, a novel method to identify the presence of attacks in UWB 802.15.4z HRP. CicadaSwat observes the Channel Impulse Response (CIR) of each received frame during ranging, and utilizes other observed signal characteristics to detect anomalies. We evaluated the performance of our model by mounting two attacks proposed by the research community, namely Cicada-TF and Adaptive Injection attacks. We verified it on a real test-bed using DWM3000 and NRF52840 Development Kit hardware, and measure its efficacy in three separate environments. CicadaSwat detects the presence of attacks with upto 94% accuracy, even higher depending upon the leading edge algorithm used.

7.1.1. Limitations

Since, the proposed model is the first solution aimed at addressing vulnerabilities in the UWB HRP PHY, it could be used as the stepping stone for further research work in this domain. Expanding the number of environments to also include outdoor and industrial locations would be useful, as they would cover more NLoS scenarios. The DWM3000 IC can only measure the approximate power levels [17], and since the hardware is currently sold as engineering samples, it is recommended that the antenna delay is calibrated according to the use case. Furthermore, the IC contains several parameters that are recommended by the manufacturer to be set after experimentation in the environment. For the purpose of this experiment, the default values were used. The device currently only supports the BPRF mode, with a PRF of 64 MHz. The performance of the proposed model needs to be evaluated for the higher PRFs such as 125 and 250 MHz. Additionally, the datasets were collected when both the transmitter and the receivers were stationary, more work is required to identify when the nodes are not static.

The lack of a Software Defined Radio (SDR) that operates within the UWB spectrum also inhibited the experiments performed, as the successful reception of a frame could only be observed by a receiver, in this case DWM3000, and verification of a successful attack was not possible until the measured distances were obtained from the metadata. The DWM3000 also does not store the received signals from the energy accumulator, and only the CIR is stored. This made observing signal characteristics while mounting attacks difficult, as the physical signals could not be recorded or observed. Furthermore, the number of 802.15.4z certified wireless ICs are severely limited, and as such all research work until now has been done using older DWM1000 hardware or similar chips. For DWM3000, there was no public information available.

7.2. Future Works

The proposed research work can be extended in multiple ways:

- The current work implements the Adaptive Injection Attack using a simulation. This is due to the lack of capable devices that lets injection of signals at a specific fraction of the transmitting frequency. A vector signal generator can be used for the creation of such radio signals. They can be used to mount physical attacks on the hardware, by transmitting very specific signals that coincide with the genuine ones.

- The three environments considered, while they provide a strong indication of the applicability of the proposed model in newer locations, however do not model all possible delay spreads as explained in the IEEE channels document for 802.15.4a. The work can be extended to include environments such as Industrial or outdoor areas with severe NLoS and for measuring the performance of the proposed model. The documents states that in certain outdoor conditions a delay spread of more than 300ns can occur. In such cases, the current model may not perform as well due to the lack of training data.
- We perform the experiments for UWB HRP in BPRF mode on the hardware. The higher values of PRF can be simulated and the performance of the model can be measured for all environments as described in the IEEE channel models document. Authors in [47] present and evaluate the success of their attacks using these simulations and environments. There is also a lack of HPRF capable devices that are available for sale.
- Currently the system utilizes two nodes to perform ranging. The verifier could measure the Channel Impulse Response using multiple tags. They could use multiple antennae that are placed in several different locations in an environment, and then utilize all the CIRs for the identification of anomalies. An adversary injecting signals into the system has lower chances of mounting the attacks without being identified.
- During experimentation, the noise threshold was low in the 8 GHz spectrum, as there were no other devices. It would be interesting to evaluate the performance of CicadaSwat when the environments contain a high density devices that communicate within this channel, or in extremely noisy conditions.
- In a system with multiple deployed verifiers, the path which the transmitter takes could also be used to verify the authenticity of each ranging session. For example, a person may be expected to pass a set of way-points while entering a building. During verification, the verifier ensures that the path taken by the transmitter adhere to these requirements.

References

[1] $£20,000$ *keyless car theft device disguised as a game boy recovered by police, 2021.* 2021. URL: `https://www.carthrottle.com/post/20000-keyless-car-theft-device-disguised-as-a-game-boy-recovered-by-police/`.

[2] *3db Access, https://www.3db-access.com*. 2020. URL: `%5Curl%7Bhttps://www.3db-access.com/%7D`.

[3] 3db Access. *Impulse Radio UWB Principles and Regulation*. 2021. URL: `https://www.3db-access.com/article/17`.

[4] G Roberto Aiello and Gerald D Rogerson. "Ultra-wideband wireless systems". In: *IEEE microwave magazine* 4.2 (2003), pp. 36–47.

[5] *Android UWB API support: https://android-review.googlesource.com/q/UWB*. URL: `https://android-review.googlesource.com/q/UWB`.

[6] *Apple Nearby Interaction, https://developer.apple.com/documentation/nearbyinteraction*. 2021. URL: `https://developer.apple.com/documentation/nearbyinteraction`.

[7] Gildas Avoine et al. "Security of distance-bounding: A survey". In: *ACM Computing Surveys (CSUR)* 51.5 (2018), pp. 1–33.

[8] David Basin et al. "Formal reasoning about physical properties of security protocols". In: *ACM Transactions on Information and System Security (TISSEC)* 14.2 (2011), pp. 1–28.

[9] Patrick Bergmans. "A simple converse for broadcast channels with additive white gaussian noise (corresp.)" In: *IEEE Transactions on Information Theory* 20.2 (1974), pp. 279–280.

[10] Stefan Brands and David Chaum. "Distance-bounding protocols". In: *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer. 1993, pp. 344–359.

[11] Agnès Brelurut, David Gerault, and Pascal Lafourcade. "Survey of distance bounding protocols and threats". In: *International symposium on foundations and practice of security*. Springer. 2015, pp. 29–49.

[12] LAN/MAN Standards Committee et al. *IEEE Computer Society: IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*. 2002.

[13] Alberto Compagno et al. "Modeling enlargement attacks against UWB distance bounding protocols". In: *IEEE Transactions on Information Forensics and Security* 11.7 (2016), pp. 1565–1577.

[14] Mauro Conti and Chhagan Lal. "Context-based Co-presence detection techniques: A survey". In: *Computers & Security* 88 (2020), p. 101652.

[15] Danny Dolev and Andrew Yao. "On the security of public key protocols". In: *IEEE Transactions on information theory* 29.2 (1983), pp. 198–208.

[16] Saar Drimer, Steven J Murdoch, et al. "Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks." In: *USENIX security symposium*. Vol. 312. 2007.

[17] *DW1000 Radio IC User Manual, https://www.decawave.com/product/dw1000-radio-ic*. Dec. 2020. URL: `%5Curl%7Bhttps://www.decawave.com/product/dw1000-radio-ic/%7D`.

[18] IBM Education. *What is Supervised Learning?* 2021. URL: `https://www.ibm.com/cloud/learn/supervised-learning`.

[19] Manuel Flury et al. "Effectiveness of distance-decreasing attacks against impulse radio ranging". In: *Proceedings of the third ACM conference on Wireless network security*. 2010, pp. 117–128.

[20] Robert J Fontana, Edward Richley, and JoAnn Barney. "Commercialization of an ultra wideband precision asset location system". In: *IEEE Conference on Ultra Wideband Systems and Technologies, 2003*. IEEE. 2003, pp. 369–373.

[21] Aurélien Francillon, Boris Danev, and Srdjan Capkun. “Relay attacks on passive keyless entry and start systems in modern cars”. In: *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Eidgenössische Technische Hochschule Zürich, Department of Computer Science. 2011.

[22] Lishoy Francis et al. “Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones.” In: *IACR Cryptol. ePrint Arch.* 2011 (2011), p. 618.

[23] Sébastien Gambs, Carlos Eduardo Rosar Kos Lassance, and Cristina Onete. “The not-so-distant future: Distance-bounding protocols on smartphones”. In: *International Conference on Smart Card Research and Advanced Applications*. Springer. 2015, pp. 209–224.

[24] Xiaojing Huang et al. “Ultra-wideband technology for video surveillance sensor networks”. In: *2006 4th IEEE International Conference on Industrial Informatics*. IEEE. 2006, pp. 1012–1017.

[25] Mohammed Husseini, Ali El-Hajj, and Christos Christodoulou. “Cognitive Radio: UWB Integration and Related Antenna Design”. In: Nov. 2010. ISBN: 978-953-307-213-5. DOI: 10.5772/10405.

[26] *IEEE 802.15.4z-2020 IEEE standard for low-rate wireless networks amendment 1: Enhanced ultra wideband (uwb) physical layers (phys) and associated ranging techniques 2021*. 2021. URL: https://standards.ieee.org/standard/802_15_4z-2020.html.

[27] *Introduction to Impulse Radio UWB Seamless Access*. URL: https://www.firaconsortium.org/sites/default/files/2020-04/fira-introduction-impulse-radio-uwb-wp-en.pdf.

[28] VP Ipatov. “Ternary sequences with ideal periodic autocorrelation properties”. In: *Radio Engineering and Electronic Physics* 24 (1979), pp. 75–79.

[29] Kyungho Joo, Wonsuk Choi, and Dong Hoon Lee. “Hold the door! fingerprinting your car key to prevent keyless entry car theft”. In: *arXiv preprint arXiv:2003.13251* (2020).

[30] Mika Juuti et al. “STASH: Securing transparent authentication schemes using prover-side proximity verification”. In: *2017 14th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE. 2017, pp. 1–9.

[31] Carlos E.R.K Lassance. “Implementing Distance-bounding protocols on Android smartphones”. PhD thesis. 2015.

[32] Patrick Leu et al. “Message time of arrival codes: A fundamental primitive for secure distance measurement”. In: *2020 IEEE Symposium on Security and Privacy (SP)*. IEEE. 2020, pp. 500–516.

[33] James Lewis, David Gerault, and Ioana Boureanu. “Here and there at once, with my mobile phone!” In: *Proceedings SECRYPT 2019: International Conference on Security and Cryptography*. Vol. 2. 2019, pp. 478–484.

[34] Andreas F Molisch et al. “IEEE 802.15. 4a channel model-final report”. In: *IEEE P802* 15.04 (2004), p. 0662.

[35] Alex Moschevikin et al. “Investigations on passive channel impulse response of ultra wide band signals for monitoring and safety applications”. In: *2016 3rd International Symposium on Wireless Systems within the Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS)*. IEEE. 2016, pp. 97–104.

[36] Hildur Ólafsdóttir, Aanjhan Ranganathan, and Srdjan Capkun. “On the security of carrier phase-based ranging”. In: *International Conference on Cryptographic Hardware and Embedded Systems*. Springer. 2017, pp. 490–509.

[37] *Police warn of rise in keyless car thefts as cctv shows thieves stealing mercedes in 60 seconds*. 2021. URL: https://news.sky.com/story/police-warn-of-rise-in-keyless-car-thefts-as-cctv-shows-thieves-stealing-mercedes-in-60-seconds-12361152.

[38] Marcin Poturalski et al. “Distance bounding with IEEE 802.15. 4a: Attacks and countermeasures”. In: *IEEE Transactions on Wireless Communications* 10.4 (2011), pp. 1334–1344.

[39] Aanjhan Ranganathan and Srdjan Capkun. “Are We Really Close? Verifying Proximity in Wireless Systems”. In: *IEEE Security & Privacy* 15.3 (2017), pp. 52–58. DOI: 10.1109/MSP.2017.56.

[40] Aanjhan Ranganathan et al. “Design and implementation of a terrorist fraud resilient distance bounding system”. In: *European Symposium on Research in Computer Security*. Springer. 2012, pp. 415–432.

[41] Kasper Bonne Rasmussen and Srdjan Capkun. “Realization of RF Distance Bounding.” In: *USENIX Security Symposium*. 2010, pp. 389–402.

[42] *Relay Attacks, Keyless car theft, https://www.which.co.uk/news/2020/05/keyless-car-theft-why-arent-car-manufacturers-doing-more/*. URL: `https://www.which.co.uk/news/2020/05/keyless-car-theft-why-arent-car-manufacturers-doing-more/`.

[43] Babins Shrestha, Manar Mohamed, and Nitesh Saxena. “Walk-unlock: Zero-interaction authentication protected with multi-modal gait biometrics”. In: *arXiv preprint arXiv:1605.00766* (2016).

[44] Babins Shrestha, Manar Mohamed, and Nitesh Saxena. “ZEMFA: zero-effort multi-factor authentication based on multi-modal gait biometrics”. In: *2019 17th International Conference on Privacy, Security and Trust (PST)*. IEEE. 2019, pp. 1–10.

[45] Babins Shrestha et al. “Contextual proximity detection in the face of context-manipulating adversaries”. In: *arXiv preprint arXiv:1511.00905* (2015).

[46] Mridula Singh, Patrick Leu, and Srdjan Capkun. “UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks.” In: *NDSS*. 2019.

[47] Mridula Singh et al. “Security analysis of IEEE 802.15. 4z/HRP UWB time-of-flight distance measurement”. In: *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2021, pp. 227–237.

[48] Mridula Singh et al. “Uwb-ed: Distance enlargement attack detection in ultra-wideband”. In: *28th USENIX Security Symposium (USENIX Security 19)*. 2019, pp. 73–88.

[49] RS Thoma et al. “UWB sensor networks for position location and imaging of objects and environments”. In: *The Second European Conference on Antennas and Propagation, EuCAP 2007*. IET. 2007, pp. 1–9.

[50] Nils Ole Tippenhauer et al. “UWB rapid-bit-exchange system for distance bounding”. In: *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. 2015, pp. 1–12.

[51] Hien Thi Thu Truong et al. “Comparing and fusing different sensor modalities for relay attack resistance in zero-interaction authentication”. In: *2014 IEEE International Conference on Pervasive Computing and Communications (PerCom)*. IEEE. 2014, pp. 163–171.

[52] Hien Thi Thu Truong et al. “DoubleEcho: Mitigating context-manipulation attacks in copresence verification”. In: *2019 IEEE International Conference on Pervasive Computing and Communications (PerCom*. IEEE. 2019, pp. 1–9.

[53] *Ultra-Wideband NXP, https://www.nxp.com/applications/enabling-technologies/connectivity/ultra-wideband-uwb:UWB*. URL: `%5Curl%7Bhttps://www.nxp.com/applications/enabling-technologies/connectivity/ultra-wideband-uwb:UWB%7D`.

[54] Juan Wang, Karim Lounis, and Mohammad Zulkernine. “CSKES: A context-based secure keyless entry system”. In: *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*. Vol. 1. IEEE. 2019, pp. 817–822.

[55] Cong Wu et al. “Liveness is Not Enough: Enhancing Fingerprint Authentication with Behavioral Biometrics to Defeat Puppet Attacks”. In: *29th USENIX Security Symposium USENIX Security 20)*. 2020, pp. 2219–2236.

[56] Ping Wen Yanzhi Ren, Zhourong Zheng Hongbo Liu, and Yingying Chen. “Proximity-Echo: Secure Two Factor AuthenticationUsing Active Sound Sensing”. In: *2021 IEEE INFOCOM*. IEEE. 2021, pp. 1–9.

[57] Jinyun Zhang et al. “UWB systems for wireless sensor networks”. In: *Proceedings of the IEEE* 97.2 (2009), pp. 313–331.