Diss. ETH No. 27823

Securing Distance Measurement against Physical Layer Attacks

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

MRIDULA SINGH

Master of Technology in Computer Science,
IIIT Delhi, India

born on 01.03.1990

citizen of India

accepted on the recommendation of

Prof. Dr. Srdjan Čapkun, examiner
Prof. Dr. Kenneth G. Paterson , co-examiner
Prof. Dr. Yongdae Kim, co-examiner

2021

Tell me and I forget. Teach me and I remember. Involve me and I learn.

— Benjamin Franklin

Dedicated to
my late father, Dr. Pramod Kumar
to whom I owe everything.

Abstract

Secure and accurate distance measurement between devices is an essential requirement of many applications, some notable applications being contactless access, tracking, and navigation. These devices exchange wireless signals to conduct distance measurements. The time the signal takes to travel from one device to another and the properties of the received signal are used for distance estimations. The techniques used for distance measurement have advanced in the last decade, providing accuracy up to decimeter level. Meanwhile, the attacker's capabilities have also advanced, especially with the availability of low-cost software-defined radios. The signal injected by an attacker can create the impression that devices are closer or further than their actual distance. An attacker can mount devastating attacks at the physical layer without breaking upper-layer security protocols. Distance modification attacks have serious implications - an attacker can gain entry into a restricted area, make fraudulent payments, steal a car, or manipulate positioning information. As the number of applications employing ranging information continues to grow, the incentive to perform distance manipulation attacks similarly increases for the attacker.

In this thesis, we analyze the security of the existing ranging systems and propose new designs with better performance, scalability, and security guarantees. First, we show that existing UWB ranging systems cannot provide performant and secure ranging systems; they trade one for another. We design *UWB with pulse reordering* (UWB-PR), the first modulation scheme that secures distance measurement between two mutually trusted devices against all physical-layer distance shortening attacks without sacrificing performance, therefore simultaneously enabling extended range and security. Second, distance enlargement attacks are prevented using verification infrastructure; however, such infrastructures are expensive, and sometimes their installation is infeasible. We present *Ultra-Wideband Enlargement Detection* (UWB-ED), a new detection technique that uses integrity checks at the signal level to detect distance enlargement attacks. Third, we show that existing LTE/5G positioning cannot be trusted to provide secure distance measurement. We develop *V-Range*, the first secure cellular (5G) ranging system capable of executing ranging operations resilient to both distance enlargement and shortening attacks. The designs we propose are fully compatible with respective UWB

and 5G standards, and they can be implemented directly on top of existing transceivers.

Zusammenfassung

Die sichere und genaue Entfernungsmessung zwischen Geräten ist eine wesentliche Anforderung vieler Anwendungen, wobei der kontaktlose Zugriff, das Tracking und die Navigation besonders nennenswerte Beispiele darstellen. Diese Geräte tauschen Funksignale aus, um Entfernungsmessungen durchzuführen. Die Zeit, die das Signal benötigt, um von einem Gerät zum anderen zu gelangen, und die Eigenschaften des empfangenen Signals werden zur Entfernungsmessung verwendet. Die dafür verwendeten Techniken haben sich in den letzten zehn Jahren gewandelt und können bis auf Dezimeter genau sein. Inzwischen haben sich auch die Fähigkeiten des Angreifers weiterentwickelt, insbesondere mit der Verfügbarkeit kostengünstiger Software Defined Radios. Das von einem Angreifer gesendete Signal kann den Eindruck erwecken, dass sich Geräte, relativ zu ihrer eigentlichen Distanz, näher oder weiter entfernt befinden. Ein Angreifer kann dabei verheerende Angriffe auf der Bitübertragungsschicht durchführen, ohne die Sicherheitsprotokolle der oberen Ebene zu verletzen. Angriffe, die zur vermeintlichen Entfernungsänderung führen haben schwerwiegende Folgen – ein Angreifer kann sich Zugang zu einem Sperrgebiet verschaffen, betrügerische Zahlungen tätigen, ein Fahrzeug stehlen oder Positionsinformationen manipulieren. Da die Zahl der Anwendungen, die Entfernungsinformationen verwenden, weiter ansteigt, steigt auch der Anreiz für solche Distanzmanipulationsangriffe in ähnlicher Weise.

In dieser Arbeit analysieren wir die Sicherheit der bestehenden Ranging-Systeme und schlagen neue Designs mit besserer Leistung, Skalierbarkeit und Sicherheitsgarantien vor. Zuerst zeigen wir, dass bei existierenden UWB-Ranging-Systemen Leistungsfähigkeit und Sicherheit in gegenseitigem Konflikt stehen. Wir entwickeln *UWB with pulse reordering* (UWB-PR), das erste Modulationsschema, das die Entfernungsmessung zwischen zwei gegenseitig vertrauenswürdigen Geräten gegen alle distanzverkürzenden Angriffe auf der Bitübertragungsschicht absichert, ohne die Leistung zu beeinträchtigen, und so gleichzeitig eine erweiterte Reichweite und Sicherheit ermöglicht. Zweitens werden Angriffe zur Entfernungserweiterung durch die Verifikationsinfrastruktur verhindert; Allerdings sind solche Infrastrukturen teuer, und manchmal ist ihre Installation nicht durchführbar. Wir präsentieren mit *Ultra-Wideband Enlargement Detection* (UWB-ED) ein neuartiges Detektionsverfahren, das Integritätsprüfungen

auf Signalebene verwendet, um Angriffe mit dem Ziel einer Entfernungserweiterung zu erkennen. Drittens zeigen wir, dass der bestehenden LTE/5G-Positionierung hinsichtlich sicherer Entfernungsmessung nicht vertraut werden kann. Wir entwickeln *V-Range*, das erste sichere Ranging-System für Mobilfunkanwendungen (5G), das Ranging-Operationen ausführen kann, welche sowohl gegen Distanzvergrößerungs- als auch -verkürzungsangriffe widerstandsfähig sind. Die von uns vorgeschlagenen Designs sind vollständig kompatibel mit den jeweiligen UWB- und 5G-Standards und können direkt auf bestehenden Transceivern implementiert werden.

Acknowledgement

When I look back at my journey from residing in a small unknown village in India to successfully defending my Ph.D. thesis, I am brimmed with a plethora of emotions. However, that one emotion that triumphs over all others is the feeling of gratefulness - a feeling that I associate with each and every person who has been a part of this journey and has made it memorable through their support, guidance, cooperation, understanding, and encouragement.

First and foremost, I would like to thank my doctoral thesis advisor - Prof. Dr. Srdjan Capkun, for all his help and guidance. He has seen me succeed and fail in equal measures and has propelled me to strive for success, no matter what. He was always very supportive and encouraged me to pursue various research topics. Moreover, I have never met a person as witty as him in my life. I aspire to be as funny, energetic, and enthusiastic as Prof. Dr. Capkun, and that someday, I would be able to command an audience as well as he can. It has been an absolute privilege and honor to be working with a person of his stature, and I look up to him to become a better person, both professionally and personally.

I would like to thank Prof. Dr. Yongdae Kim and Prof. Dr. Kenneth G. Paterson for accepting my request to be a part of my dissertation committee and setting their precious time aside to review my thesis.

In the last five years, I have had the opportunity to meet and team up with some of the brightest minds in the field of Wireless Security, namely, Prof. Dr. Aanjhan Ranganathan, Prof. Dr. AbdelRahman Abdou, and Dr. Marc Röschlin. I am very grateful to them; these people also coached me from time to time, helping me identify my shortcomings and encouraging me to build on my strengths. Another person that deserves mention here is Dr. Boris Danev. He was one of my first go-to person when I joined ETH Zurich. I would always treasure his guidance which made me look at things from a different perspective.

Staying this far away from home can be challenging, but what made me feel closer to family was my colleague Aritra Dhar. From getting used to the new place of work, exploring the new city, catching up for Indian food over the weekend, Aritra has been there all way long! Having knowledgeable people around you is good, but what is better is to have a fun-loving office mate, who was none other than Patrick Leu. I admire him for his ability to incorporate various topics into a single discussion. Some works that we

did together have had a high impact on the outcome of this thesis which I will always remember.

I thank my colleagues David Sommer and Dr. Sinisa Matetic for always making me feel more comfortable in the group. I also thank Ivan Puddu, Moritz Schneider, Karl Wust, Dr. Enis Ulqinaku, Der-Yeuan Yu, Daniele Lain, Dr. Hubert Ritzdorf, Dr. Kari Kostiainen, and Dr. Luka Malisa for making my journey truly memorable. The discussions that we have had over lunch were truly inspiring. Thank you, Lara Schmid, for always lifting me with your kind words. I also thank Mrs. Barbara Pfändner, Saskia Wolf, and Viven Klomp for all the support and help with administrative matters over the years. I would also like to thank the CSNOW team for helping me become a better leader.

I would also like to thank Prof. Dr. Huzur Saran, Prof. Dr. Vinay Ribeiro, Prof. Dr. Sanjit Krishnan Kaul, Dr. Koustuv Dasgupta, and Dr. Kuldeep Yadav for having a great influence on the choice I made for my studies and professional path.

Last but not least, I would like to extend my gratitude towards my family and other friends back in India for their immense support. My parents and my sisters have always taught me to have a clear vision in life and have backed me to reach for bigger achievements in life. A big thank you to my lovely boyfriend - Saurav Bose, for his words of encouragement, unconditional love, and support. And not to forget, a special thank you to my best friends - Akanksha Rastogi and Aparna Sarswat, for always being there to listen to me.

Finally, I would like to dedicate my doctoral dissertation to my late father - Dr. Pramod Kumar. He was one of the first few people who understood my knack for research and did everything possible within his capacity so that I could pursue my dreams. He has taught me how to persevere and never back down during precarious situations. Back in 2016, he was again the first one, encouraging me to go for Ph.D. If there was anyone with whom I would have first shared the news of my successful dissertation, that would have been my father. He would have been the proudest!

Contents

List of Figures

List of Tables

Chapter 1
Introduction

Measuring the relative distance between devices is often necessary for a variety of modern-day applications. The use of contactless tokens has been accepted as a means of executing money transactions [1], unlocking digital devices [2, 3], providing access to infrastructure [4, 5], and verifying credentials using electronic passports [6]. The demand for ranging information is increasing for autonomous and cyber-physical systems; a stringent requirement for these systems is to avoid crashing into, for example, buildings, pedestrians, properties, or each other [7, 8]. Keeping autonomous vehicles and drones on their intended paths and preventing their collision can be achieved if they are able to calculate their relative distances accurately and securely.

Ranging systems are in more demand than ever due to the ongoing COVID-19 pandemic. Contract tracing apps, where distance is measured between co-located mobile devices, facilitate the public, social organizations, and government to prevent and control the pandemic. These apps are a healthy supplement to manual tracing in which human workers interview people who have been diagnosed with COVID-19 and then track down their recent contacts [9, 10, 11]. The use of contactless access tokens has also seen a significant increase. This growth is not particularly surprising due to the variety of benefits contactless transactions provide. More so than ever, users are focused on reducing physical contact at the point of sale for health and safety purposes, and contactless payments allow them to purchase goods without having to physically enter their personal identification number on payment terminals [12, 13, 14].

The use of ranging information in a variety of applications makes it a target of attackers with different motivations. Distance manipulation attacks have led to car thefts, unauthorized payment execution, and location coordinates manipulation. It is therefore essential to explore the current distance measurement systems' performance and security guarantees. Use cases like contactless access tokens generally need to establish an upper bound on the measured distance. Upcoming use cases like autonomous vehicles demand measured distance to be exact, *i.e.,* device should establish both upper and lower bound on the measured distance.

Distance manipulation attacks are performed by manipulating the logical or physical layer. While logical-layer attacks manipulate message

bits, physical-layer attacks involve manipulating signal characteristics to incorrectly measure the signal's phase, amplitude, frequency, or arrival time. Some of the most notable attacks, such as relay attacks on signal strength-based ranging systems, are conceptually simple to perform with limited or no technical knowledge [15, 16]. The adversary simply amplifies the signal close to the transmitter until the received signal strength is consistent with the expected path loss over the claimed distance. Researchers have repeatedly demonstrated the vulnerability of passive keyless entry systems of automobiles to the relay attack [17]. Attackers were able to steal the car by relaying the signal between the car and the key when they were several tens of meters apart [16, 18].

The majority of research on enabling secure distance measurement is focused on upper bounding measured distance using logical layer cryptographic protocols known as distance bounding protocols [19, 20, 21, 22, 23, 24]. These challenge-response protocols measure the time-of-flight (ToF) of cryptographically generated data bits and use this transmission time for distance estimation. These protocols provide an upper bound on the physical distance between two communicating parties, armed by the fact that an adversary fails to guess (secret) bit-level information, thereby preventing distance-shortening attacks. Systems using distance bounding protocols are inherently secure against distance shortening by relay attacks, as a relay by definition extends the ranging distance. Although essential, such protocols are not sufficient to achieve secure ranging; the possibility of physical layer attacks still exists. For example, an attacker can trick the receiver into incorrect arrival time estimation by predicting the symbol's inner signal structure. So far, using a single ultra-wideband (UWB) pulse to represent one bit of information is the only physical layer design that prevents all known physical layer attacks. However, this design is performant only under short-range in line-of-sight (LoS) channel conditions.

Distance enlargement, where the measured distance is longer than the actual distance, is more devastating than the reduction attack. An adversary in the communication range only needs to annihilate (cancel) [25] or distort the authentic signals to prevent the receiver from identifying them and using them for distance estimation. The attacker can replay a delayed version of the legitimate signal, The attacker can replay a delayed version of the legitimate signals, which it has already received by positioning itself in the sender's vicinity, to create an impression of long distance between devices. The adversary need not guess these signals nor compromise any upper-layer protocols to do that. In a collision-avoidance system of automobiles or self-

driving cars, distance enlargement by a few meters ($\sim$ a few nanoseconds) could be catastrophic; it can deviate vehicles from their intended paths or cause physical collisions. There is no approach to find a lower bound on the measured distance or detect the possibility of the enlargement attack between two devices. Existing protection approaches rely on dense and often fixed verification infrastructures, *e.g.,* towers. These may not exist and often do not; installing them in outdoor settings is expensive and not necessarily feasible (*e.g.,* in drone-based military missions behind enemy lines).

The applications that use ranging information is increasing, especially given the recent advent in autonomous systems, robots, contactless access tokens, contact tracing, and many more cyber-physical systems. With these advancements, the attacker's motivation to perform distance manipulation attacks is only bound to increase. Therefore, there is a need to ensure these systems' resilience against distance manipulation attacks. This need has motivated academia and industry alike to introduce secure positioning in the upcoming standards, including IEEE 802.15.4z (ultra-wideband), IEEE 802.11az (WiFi), and 3GPP 5G. The core of this thesis is to find shortcomings of the existing ranging systems and propose new designs to provide secure, scalable, and performant ranging systems.

1.1 Contributions

As mentioned above, distance modification attacks have serious implications; an attacker can gain entry into a restricted area, make fraudulent payments [26, 27], steal a car [17], or manipulate positioning information [28]. The logical layer distance bounding protocols prevent relay attacks, but they fall short when an attacker can perform physical layer attacks or intends to perform distance enlargement. Existing ranging systems are not capable of providing performance and security against distance reduction attacks; they achieve security through short symbol lengths and sacrifice performance (i.e., limit the maximum distance of measurement and channel conditions), or use longer symbol lengths, therefore sacrificing security. The requirement of the enlargement attack prevention is averted by the use of verification infrastructure (*i.e.,* verifiable multilateration) – the device's distance is measured from at least three reference points and assumed that none of the measured distance is shortened. In this thesis, we discuss the security of existing ranging systems (*i.e.,* IEEE 802.15.4z LRP and HRP, WiFi FTM, and LTE/5G PRS) under known and previously unexplored attacks. By hiding bit to pulse

mapping using pulse reordering, we designed the first UWB ranging system that achieves security and longer symbol (performance under longer distance and NLoS conditions). Using integrity checks at the receiver, we show the possibility of detecting enlargement attacks at the physical layer, preventing the need for verification infrastructure. We design the first secure physical layer compatible with the 5G system, enabling secure and accurate ranging for a wide range of applications. We show that modulation scheme, channel conditions, and receiver design directly affect the performance and security of the system. The designs we propose are secure candidates for the Message Time of Arrival Codes (MTAC), a fundamental primitive that ensures distance measurement security from all known physical layer attacks.

Secure and Performant Ranging. The UWB ranging systems follow IEEE 802.15.4a/f/z standards. IEEE 802.15.4z has been finalized recently in 2020 and has enhanced the existing IEEE 802.15.4a and IEEE 802.15.4f standard with new integrity features for distance measurement. We show that even after these enhancements, the modes proposed in IEEE 802.15.4z cannot provide secure and performant ranging. For example, extended and long-range mode configurations of LRP are still vulnerable to distance manipulation attacks due to the predictable symbol structure. Therefore, LRP mode needs to choose between security and extended distance. HRP mode, on the other hand, has hard security and performance tradeoff; HRP mode cannot provide secure ranging if performance in benign NLoS scenarios is equally important. Therefore, these ranging systems are limited to short-range LoS conditions. Many applications demand range estimation in the long-range and NLoS conditions; for example, a user should be able to unlock her car if the key fob is inside her pocket.

We present UWB with pulse reordering (UWB-PR), the first modulation scheme that secures distance measurement between two mutually trusted devices against all physical-layer distance shortening attacks without sacrificing performance, therefore simultaneously enabling extended range and security. We analyze the security of UWB-PR under an attacker that fully controls the communication channel and show that UWB-PR resists such strong attackers. We evaluate UWB-PR using a UWB system built on top of the IEEE 802.15.4 device and show that it achieves distances of up to 93m with 10cm precision (LoS). Finally, UWB-PR shows that secure distance measurement can be built on top of modulation schemes with longer symbol lengths - so far, this was considered insecure. UWB-PR is,

therefore, a good candidate for the extended mode of the new 802.15.4z Low Rate Pulse standard.

Enabling Enlargement Attack Detection. Existing distance measurement techniques are incapable of protecting against adversarial distance enlargement—a highly devastating tactic in which the adversary reissues a delayed version of the signals transmitted between devices, after distorting the authentic signal to prevent the receiver from identifying it. The adversary need not break crypto or compromise any upper-layer security protocols to mount this attack. So far, the system relies on the verification infrastructure to detect distance enlargement attacks - at any time, at least three verification nodes should surround the device to prove that distance is not enlarged. Using verification infrastructure has additional expenses and overhead.

We present Ultra-Wideband Enlargement Detection (UWB-ED), a new modulation technique to detect distance enlargement attacks and verify distances measurement between two mutually trusted devices. We show that a combination of secure code generation with data and signal level integrity checks at the receiver is required to detect legitimate distorted signals. We validate our design using simulations under different channel conditions and show that UWB-ED is a good candidate for 802.15.4z Low Rate Pulse.

Secure Cellular (5G) Ranging. The standardization units have incorporated ToF ranging in widely-used communication systems. For example, IEEE 802.11mc specified Fine Time Measurement (FTM) for WiFi, 3GPP specified Positioning Reference Signal (PRS) for cellular communication (LTE/5G). The systems based on these standards are commercially available, and APIs to access ranging information are available to developers, allowing their use in new, feature-rich, safety- and security-critical applications. We analyze these systems across physical and logical layers and show that an external adversary can manipulate distances to any arbitrary value. Distance bounding protocols can prevent logical layer attacks, but the physical layer has fundamental limitations. Orthogonal frequency-division multiplexing allows distance manipulation due to longer symbol duration, and the receiver cannot differentiate the attack signal from multipath. These systems use coherent receiver design, allowing distance enlargement by an indirect attack, where an attacker manipulates information needed to decode the data, such as carrier frequency offset estimation.

3GPP has put forward a plan to introduce positioning and ranging into 5G, and new waveforms are under development [29, 30, 31, 32, 33]. We enumerate the challenges that need to be addressed to enable secure positioning in 5G. We propose V-Range, the first secure ranging system for 5G-NR radio architecture, and demonstrate that this system is secure against distance reduction and enlargement attacks. The modification we propose to the current 5G transceivers can be deployed extensively through firmware updates. We build a proof-of-concept for sub-6GHz and mm-wave modes of 5G communication and evaluate their performance and security guarantees.

1.2 Thesis Organization

This doctoral dissertation is organized into two main parts. We begin the thesis with an overview of existing ranging techniques, known distance manipulation attacks, and primitives for the secure ranging in Chapter 2.

The first part of the thesis analyzes existing UWB ranging systems and proposes designs that prevent distance and manipulation attacks. In Chapter 3, we explore the performance and security tradeoff of the UWB ranging systems and show that we cannot trust distance measurement using these modes if we optimize them for the performance. We show that hiding pulse polarity from the attacker is not sufficient to achieve secure ranging. In Chapter 4, we present UWB-PR, a modification of IEEE 802.15.4f modulation to achieve a secure and performant ranging system. UWB-PR uses low repetition pulse with pulse reordering and distance commitment to achieve security against physical layer distance reduction attacks. In Chapter 5, we propose UWB-ED, a modulation scheme that uses integrity checks at the receiver, along with the secure physical layer designs, to detect distance enlargement attacks. This scheme detects enlargement attacks without requiring any verification infrastructure.

In the second part of the thesis, we analyze the security of OFDM-based ranging systems and propose a secure alternative. In Chapter 6, we expose vulnerabilities of the WiFi FTM and LTE/5G PRS and explain the fundamental limitation of using predictable logical layer data and OFDM symbols at the physical layer. We identify that the cellular ranging systems are vulnerable to distance enlargement by indirect attacks; an attacker manipulates the information needed to recover legitimate data, such as carrier-frequency offset estimate. In Chapter 7, we develop V- Range, the first secure ranging system that is fully compatible with 5G standards and can be implemented directly on top of existing 5G-NR transceivers. V-

Range is capable of executing ranging operations resilient to both distance enlargement and reduction attacks.

Finally, we conclude the thesis in Chapter 8 with a summary of our findings and present possible future work.

1.3 Publications

This work is mainly based on the following publications

1. Mridula Singh, Patrick Leu, Srdjan Capkun, *"UWB with Pulse Reordering: Securing Ranging against Relay and Physical Layer Attacks"*, in Network and Distributed System Security Symposium (NDSS), 2019

2. Mridula Singh, Patrick Leu, AbdelRahman Abdou, Srdjan Capkun, *"UWB-ED: Distance Enlargement Attack Detection in Ultra-Wideband"*, in USENIX Security Symposium, 2019.

3. Mridula Singh, Marc Roeschlin, Aanjhan Ranganathan, Srdjan Capkun, *"V-Range: Enabling Secure Ranging in 5G Wireless Networks"* (under review)

In addition, during my Ph.D., I co-authored the following publications. Some parts of these publications are used in this thesis.

1. Patrick Leu, Mridula Singh, Marc Roeschlin, Kenneth G. Paterson, Srdjan Capkun, *"Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement"*, in IEEE Symposium on Security and Privacy (S&P), 2020

2. Domien Schepers, Mridula Singh, Aanjhan Ranganathan, *"Here, There, and Everywhere: Security Analysis of Wi-Fi Fine Timing Measurement"*, in Security and Privacy in Wireless and Mobile Networks (WiSec), 2021

3. Mridula Singh, Marc Roschlin, Ezzat Zalzala, Patrick Leu, Srdjan Capkun, *"Security Analysis of IEEE 802.15.4z/HRP UWB Time-of-Flight Distance Measurement"*, in Security and Privacy in Wireless and Mobile Networks (WiSec), 2021 (received Distinguished Paper Award)

Chapter 2
Background RF Ranging Systems

Accurate and secure ranging is a crucial requirement for many applications. In the last decade, ranging techniques have advanced to provide decimeter-level precision. At the same time, attacker's capabilities have advanced. An attacker can buy low-cost attack setups and inexpensive software-defined radios to perform distance manipulation attacks [15, 34].

Broadly, there are two types of radio-frequency ranging systems. One set of ranging systems compute distances by measuring one or more physical properties of the signal, such as received signal strength [35], multicarrier phase ranging [36], frequency modulated continuous wave radars *etc.* Although simple to implement, these systems are susceptible to channel interference effects and require extensive error correction. Alternatively, ranging systems can compute distance by measuring time-of-flight [37, 38, 39]. A signal's time to travel from one device to the other is directly proportional to the distance, as radio waves are assumed to propagate at the constant speed of light. Hence, to measure distance, the receiver only has to determine the point in time at which the signal arrived [40, 41, 42]. This operation is called *leading edge detection*, and it works by continuously sampling the incoming signal to determine the beginning of the expected signal. The received signal is affected by multipath, fading, and attenuation, thereby making leading-edge detection challenging.

Passive Keyless Entry and Start (PKES) systems and other contactless tokens generally use signal strength to estimate proximity, but some of them are now transitioning to two-way ToF measurement using UWB ranging [43, 44, 45]. Navigation systems, such as Global Positioning System (GPS), use broadcast signals, and receivers locate themselves by calculating the time difference of arrival (TDoA) for the signal originated from different satellites. Cellular positioning using Position Reference Signal (PRS) also uses the same concept by observing the time difference of signal arriving from neighboring basestations [39].

Most of these techniques, if not designed securely, are vulnerable to logical and physical layer attacks. An attacker can fake received signal strength and phase using simple relay attacks (amplify/delay and forward) [17, 46]. The instances of cars stolen by relay attacks have appeared in many news articles [18, 16], and such relay setups can cost as little as 20$ [47]. Researchers have shown that even critical documents like electronic passports are vulnerable to these attacks [6]. Attempts have

been made to secure them by reducing the transmit power, combining data from multiple sensors, and two-factor authentication [48, 49, 50]. The GPS, although widely used, is susceptible to replay attack. An attacker can spoof GPS to change the course of a ship or force a drone to land in a hostile area [51, 52, 53, 54, 55, 56, 28].

Two-way ToF has emerged as an approach to achieve high precision and secure ranging [57, 58]. The existing research focuses on enabling security using logical layer cryptographic protocols - distance bounding protocols that return an upper bound on the measured distance, assuming that an attacker cannot guess bit level information. However, these protocols fall short if an adversary is capable of performing physical layer attacks [59, 60, 61].

In this chapter, we provide a brief overview of the Radio Frequency (RF) based ranging systems and related work. Section 2.1 describe distance measurement techniques. Section 2.2 provides an outline of the threat model that we consider throughout this thesis. In Section 2.3, we discuss different categories of distance manipulation attacks and possible defense mechanisms. Section 2.4 provides an overview of the principles and security primitive for enabling security ranging against all known physical layer attacks. Section 2.5 provide a brief summary.

2.1 Distance Measurement Techniques

We focus on the scenario where two devices in a wireless network, referred to as the verifier and the prover, are interested in securely measuring the physical distance. The techniques these devices use for distance measurement can be classified into two categories. (i) Indirect ranging – techniques that determine distance by measuring one or more physical properties of the received signal. (ii) Direct ranging – techniques that compute distance by measuring the arrival time of the signal. In this section, we give an overview of the different ranging techniques.

2.1.1 Indirect Distance Measurement

The radio signal experiences loss in signal strength and change in the phase as it travels through space. Loss in signal strength is proportional to the square of the distance between the transmitter and the receiver. The exact distance d is calculated based on the following free space path loss equation:

$$d = \frac{4}{\lambda}\sqrt{\frac{P_t G_t G_r}{P_r}}$$

λ is the signal's wavelength, P_t and P_r are the transmitted and the received signal power, G_t and G_r are the antenna gains of the transmitter and the receiver, respectively. In reality, the radio signal experiences additional losses due to its interaction with the objects in the environment (*e.g.,* reflections off buildings), which are difficult to account for accurately and directly affect the computed distance's accuracy. We currently use many signal strength-based ranging systems, including contactless payment, PKES of various automobiles, bluetooth proximity tags, and contract tracing apps [62, 63].

Similarly, the received signal's phase can also provide a distance estimate. The verifier begins ranging by transmitting a continuous wave carrier signal, while the prover locks its local oscillator to this incoming signal and transmits it back to the verifier. The verifier measures the distance (d) based on the difference in the phase (θ) of the received signal and its own reference signal. If the distance between the verifier and the prover is less than the signal's wavelength, it is calculated as,

$$d = \frac{\theta \cdot c}{4\pi \cdot f}$$

where c is the speed of light, and f is the frequency of continuous-wave carrier signal. In order to unambiguously measure distances greater than the signal's wavelength, it is necessary to keep track of the number of whole cycles elapsed. The need for keeping track of the cycles can be eliminated by using multicarrier phase ranging. Due to low-complexity and low power requirement, multicarrier phase ranging (e.g., Atmel AVR2152) is a cost-optimized solution for a wide variety of applications, including positioning of ultra-high frequency RFID systems [64]. Furthermore, carrier phase information can be accessed directly from the network cards, provide centimeter-level precision and thereby enabling its use in the indoor localization systems [65, 36].

2.1.2 Direct Distance Measurement

An alternative approach for estimating distance is by measuring the time taken by the signal to travel from the verifier to the prover. The distance (d) between the verifier and the prover can be expressed mathematically using the equation

$$d = (t_2 - t_1) \cdot c$$

where c is the speed of light, t_1 and t_2 represent the time of transmission and reception of the signal, respectively. In addition to the precise knowledge of

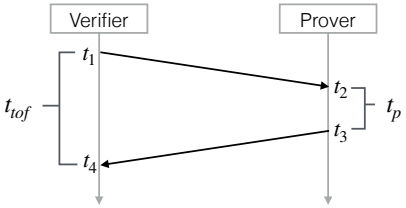


Figure 2.1: Two Way Ranging

the transmission and reception times, one-way time-of-flight measurement requires tight clock synchronization between the verifier and the prover. Note that 1 *ns* error in synchronization would result in $\approx 30\ cm$ error in the estimated distance. Given the instability of local clocks and the difficulty of achieving synchronization with nanosecond precision, most time-of-flight ranging systems compute round-trip time instead of a one-way time of flight. As shown in Figure 2.1, the verifier estimates the time elapsed between transmitting a ranging data packet and receiving an acknowledgment back from the prover. The distance between verifier and prover is therefore given by the following equation

$$d = \frac{((t_4 - t_1) - (t_3 - t_2)) \cdot c}{2}$$

Leading Edge Detection: The accuracy of the measured distance depends on the accuracy of measuring arrival time ($t2$ and $t4$) of the messages exchanged between the verifier and the prover; *i.e.,* detecting the first path/instance of the signal at the receiver. The signal used for ToA estimation is generally predictable for the receiver (also for the attacker), *e.g.,* preamble in UWB, training sequence in WiFi, and Positioning Reference Signal in 4G/5G. In order to estimate arrival time, the receiver performs cross-correlation between the received and the expected signal. As shown in Figure 2.2, the strongest correlation peak does not always represent the first occurrence of the signal at the receiver. This can be due to the fact that (i) the devices are not within LoS of each other, or (ii) an indirect path experiences constructive interference leading to a higher peak than the direct path. Therefore, after acquiring the strongest correlation peak, the receiver searches within the backsearch window a peak that satisfies noise thresholds such as peak to average power ratio [40, 41]. The accuracy, therefore, depends on various factors,

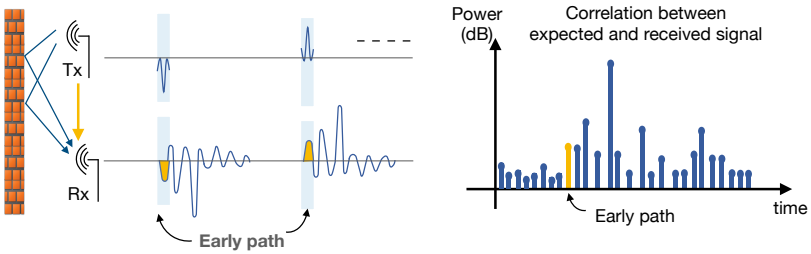


Figure 2.2: Leading edge detection algorithms search for the first occurrence of the signal at the receiver. The strongest signal does not always represent the signal arriving through the direct path.

including physical layer design, system bandwidth, channel conditions, and detection thresholds used by the leading edge algorithm.

Many systems are currently adopting ToF as the standard technique for distance measurement. WiFi devices supporting IEEE 802.11mc are capable of performing two-way ranging using Fine-timing-measurement protocol [66], enabling newer applications such as personnel management and geo-fencing. Similarly, approaches based on Observed-Time Difference Of Arrival (OTDOA) are integrated into cellular communication [39]. UWB-IR ranging is standardized in IEEE 802.15.4z and is commercially available [37, 67, 38], expediting its adoption in the automobiles and smartphones [68, 69, 43].

2.2 Threat Model

Throughout this thesis, the verifier and the prover are interested in securely measuring physical distance between them and protecting measurement from a third-party adversary. As shown in Figure 2.3, the attacker's objective is to manipulate distance measurement between the verifier and the prover; this attacker model is also known as Mafia Fraud [19]. For example, Figure 2.4 shows a rogue device (vehicle, drone, or roadside attacker) modifying the measured distance between two cars. A car may accelerate and collide if the measured distance is enlarged, and reducing the measured distance will trigger emergency brakes. There exist other frauds where prover is considered malicious or compromised [70, 71], we trust the prover in our work.

We consider Dolev-Yao's attacker [72], the attacker cannot directly modify messages exchanged between the verifier and the prover; it can rather inject signal to manipulate properties of the legitimate signal or its

Figure 2.3: In Mafia Fraud, an external attacker reduces the distance measured between two mutually trusted parties.

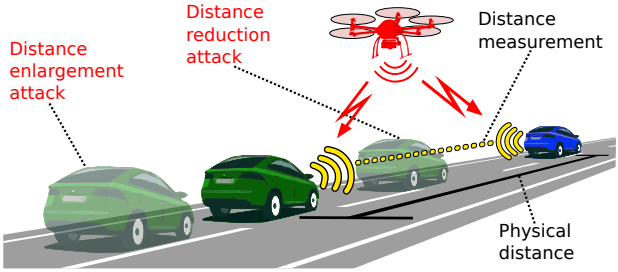


Figure 2.4: Example scenario. Distance reduction can result in unexpected emergency braking and evasive maneuvers. Distance enlargement can even lead to a collision.

arrival time. This model captures the capabilities of MITM attacks and is commonly used to assess the security of wireless protocols [73, 74]. The attacker cannot predict cryptographically generated data but knows about the protocols used for distance estimation. We assume that the attacker can transmit, eavesdrop, intercept, record, and replay arbitrarily strong radio frequency signals. An attacker can neither block the legitimate signal from arriving at the receiver, nor send it faster due to physical constraints and laws of physics. The attacker has access to the signal samples that have left the legitimate antenna after an observation delay of a few nanoseconds. Observation delay may occur due to the attacker's location and hardware constraints. We assume that the attacker has access to all samples unaffected by channel conditions, for example, by placing the attack device close to legitimate transmission. Therefore, an attacker can resolve the amplitude and phase of each sample. This is not always true for the legitimate receiver, as it receives the signal affected by channel conditions.

We assume that the attacker knows the actual physical distance between devices at any point in time. An attacker can, therefore, precisely align the transmission of the legitimate and the attack signal. The attacker's sampling rate needs to be sufficient to recover the signal. For an attack to be effective, we don't need to assume that the attacker has a higher bandwidth

since we assume the attacker can precisely synchronize to the start of the signal. However, this includes attackers that operate with multiple (smart) antennas or increase noise levels at the legitimate receiver. Finally, we consider that the attacker cannot physically tamper with the device nor compromise their firmware in any other way.

2.3 Distance Manipulation Attacks

Designing a secure ranging system is an intricate task. Most ranging systems that we use today are vulnerable to distance manipulation attacks. The distance manipulation attacks can be categorized into two broader categories. (i) *Distance reduction attack* - an adversary proves that verifier and prover are closer than their actual distance. (ii) *Distance enlargement attack* - an adversary proves that verifier and prover are farther than their actual distance. An adversary can have different incentives to reduce or enlarge the perceived distance between verifier and prover, such as opening a car, gaining access to an office, stealing money from a credit card, forcing collision between autonomous vehicles, manipulating location information *etc.* An adversary can perform distance manipulation attacks by compromising the logical or the physical layer of the ranging systems.

2.3.1 Logical Layer Attacks

The logical layer represents bit-level information exchanged between the verifier and the prover. These bits should be generated cryptographically, irrespective of the underlying physical layer and distance measurement techniques (*i.e.,* signal strength, phase, and ToF). Otherwise, it would be trivial for an unauthorized device to generate ranging signals and appear legitimate to the verifier. In Section 6.1, we will demonstrate a logical layer attack on the FTM protocol. Previous research has shown that attacks at the logical layer can be thwarted using distance bounding protocols [19, 20, 75, 23, 76, 77].

Distance Bounding Protocols: Distance bounding protocols have been extensively studied and a number of protocols were proposed and analyzed for location verification [78], wormhole attack detection [79], key establishment [80] and access control [81]. These challenge-response protocols rely on ToF measurements and provide an upper bound on the physical distance between two communicating parties, therefore, preventing distance-reduction attacks. Distance-bounding protocols send

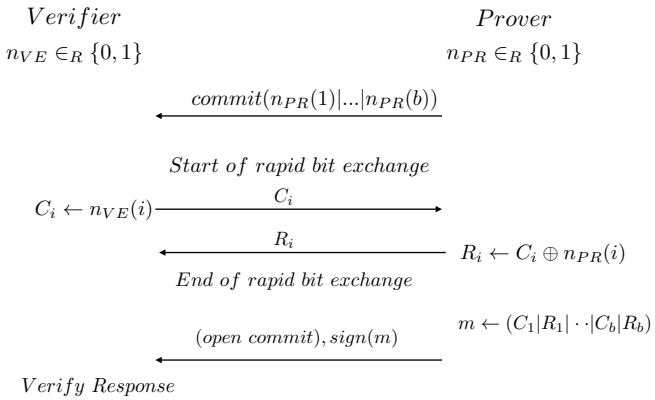


Figure 2.5: The Brands-Chaum distance-bounding protocol provides security against Mafia Fraud at the logical layer.

cryptographically generated challenges and expect a correct response within a specific time window. Brands and Chaum proposed the first distance-bounding protocol (illustrated in Figure 2.5) to prevent distance reduction from an external attacker (*i.e.,* Mafia Fraud) [19]. In this protocol, the verifier challenges the prover with a random nonce n_{VE} and measures the time until it receives the response determined using n_{PR}. This time is then converted into an upper bound on the distance between the verifier and the prover.

The attacker cannot trivially reduce this distance - unless it can guess nonces n_{VE} or n_{PR}, longer nonces lower an attacker's chances of guessing all bits. However, an attacker can trick the prover (resp. verifier) into measuring an earlier arrival time of n_{VE} (resp. n_{PR}) by physical-layer attacks. The success of the physical-layer attacks depends on the underlying modulation scheme and transceiver design. In addition to that, these protocols do not ensure security against distance enlargement attacks. An attacker can always send n_{VE} (resp. n_{PR}) after a certain delay, such that the measured distance is longer than the actual distance. It is worth noting that distance bounding protocols are the first line of defense against distance manipulation attacks, but they are insufficient to prevent attacks that we explore next.

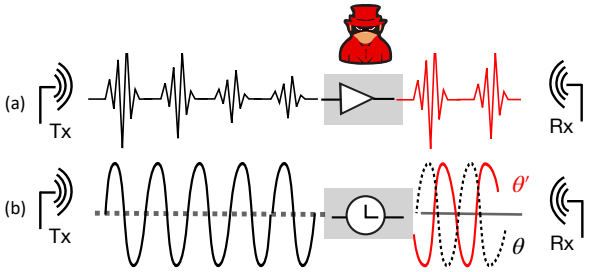


Figure 2.6: Relay attacks on the ranging systems.

2.3.2 Physical Layer Attacks

As discussed above, the distance is measured using the properties of the received signal or its arrival time. Therefore, an attacker capable of influencing them can manipulate distance estimation. The cryptographic protection at the logical layer does not guarantee security when an attacker directly exploits the physical layer.

Manipulating properties of the signal: The relay attack is a classic example of exerting control over the physical properties of the signal. Specifically, an adversary feeds the signal through an alternative propagation path and controls signal strength, phase, frequency, and arrival time. For example, to attack a signal strength-based ranging system, an attacker can simply attenuate or amplify the signal transmitted by the prover before relaying it back to the verifier. As shown in Figure 2.6a, the attacker amplifies the signal close to the transmitter until the received signal strength is consistent with the expected path loss over claimed distance. Similarly (Figure 2.6b), the signal phase can be manipulated by the attacker in order to be consistent with the expected phase. Relay attacks are conceptually simple and have been successfully performed in a number of systems, including WiFi [82], PKES systems [17], NFC [83], and Atmel AT86RF233 [84].

Ultrasonic ToF based ranging systems are also vulnerable to relay attack, an attacker can gain the advantage by relaying messages over faster RF channel [85]. However, radio waves traveling at the speed of light cannot be sent faster by the attacker. Therefore, any ToF system relying on radio waves traveling at the speed of the light is inherently resistant to distance reduction by relay attack, no matter the capability of the relay (*e.g.,* it

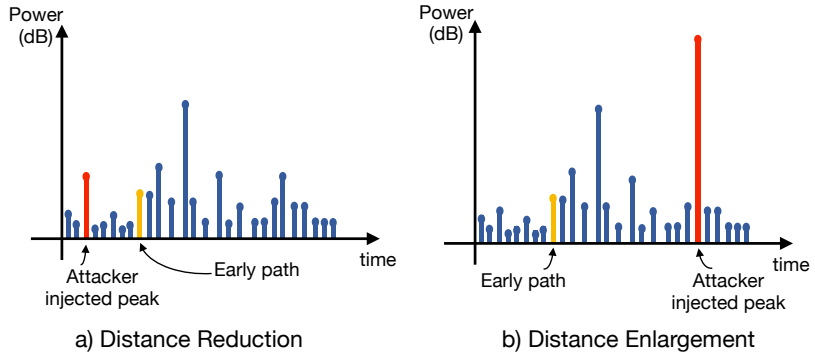


Figure 2.7: An attacker injects a peak earlier or later than the early/direct path to perform distance reduction or enlargement attacks, respectively.

being duplex or not). Therefore, the relay attack cannot reduce measured ToF, but it can increase ToF to extend the perceived distance between two legitimate devices.

Defense: By using relay attacks, an attacker can reproduce properties of the legitimate signal. Therefore, relying only on signal properties is not sufficient to design a secure ranging system [86]. However, as we show in the secure design proposed later in this thesis, the properties of the signal (signal strength and phase), when combined with ToF measurement, are instrumental in detecting distance enlargement attacks to detect traces of the legitimate signal.

Manipulating ToA estimation: The distance measurement accuracy depends on finding the first path/instance of the signal's arrival at the receiver. Therefore, an attacker can manipulate ToA estimation by injecting a path earlier or later than the early path to perform distance reduction and enlargement, respectively (Figure 2.7). These attacks exploit the fundamental difficulty in distinguishing signals arriving through the direct path from interference. Furthermore, an attacker can achieve distance enlargement by replaying the legitimate signal with higher power after a certain delay (*i.e.,* signal replay/overshadowing), such that the attack signal overlaps with the legitimate signal [87]. An attacker succeeds in distance enlargement if the signal arriving through the direct path is hidden under noise, and the attack signal is used for

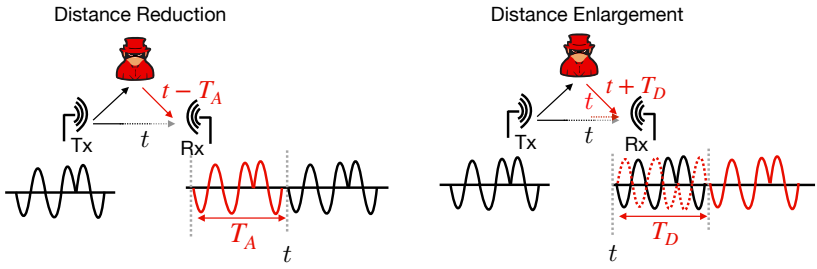


Figure 2.8: An attacker can perform distance reduction by sending the symbol earlier by time T_A. An attacker can distort the legitimate signal and then replay it after the delay T_D to perform distance enlargement.

distance estimation. GPS spoofing is classic example of manipulating ToA estimation - the attacker replays counterfeit GPS signal such that it overrides the weaker but legitimate satellite signal [88, 56]. We explore the possibility of similar attacks on WiFi FTM and cellular positioning in Chapter 6.

In systems using distance bounding at the logical layer to achieve secure distance measurement, the arrival time of cryptographically generated data bits is used for distance measurement. In such scenarios, an adversary needs to predict the inner structure of the symbol to send it in advance or annihilate it, as shown in Figure 2.8. An attacker can perform the Early Detect Late Commit (ED/LC) attack, as shown by Flury *et al.* on IEEE 802.15.4a UWB, allowing distance reduction up to 140 m [61, 60]. Aanjhan *et al.* demonstrated that 802.15.4a Chirp Spread Spectrum is also vulnerable to ED/LC attack, allowing distance reduction up to 150 m for typical short chirp durations and more than 700 m for longer chirps [89]. The systems using Orthogonal Frequency-Division Multiplexing (OFDM), including WiFi and 5G, are also vulnerable to such attacks [90].

Even when bits are generated cryptographically, it is easier to perform a distance enlargement attack. Specifically, the attacker's objective is to prevent the legitimate signal detection so that receiver uses replayed copy of the legitimate signal for bit detection. An attacker can elevate noise level (which can be detected by the receiver) or perform signal annihilation to prevent legitimate signal detection. An attacker can also use indirect means, for example, by manipulating information needed for data demodulation, such as carrier frequency offset estimation. We explore enlargement attacks in context of UWB in Chapter 3 and OFDM in Chapter 6.

Defense: To perform distance enlargement attacks, an attacker can always replay the legitimate signal after a delay with a higher power such that the attacker's injected peak is strongest. Additionally, the attacker can prevent early legitimate path detection during backsearch by injecting noise on the channel, *e.g.,* PAPR threshold cannot detect authentic peak if the noise level is elevated. Currently, there is no approach to differentiate the attacker's injected peak from the legitimate strong peak. On the other hand, distance reduction attacks by ToA manipulation can be prevented by limiting the backsearch window, but at the cost of performance, *i.e.,* legitimate direct path signal is discarded if the receiver locks on to the strong signal and does not perform backsearch.

A short symbol to represent a bit with rapid bit exchange is considered secure against ED/LC and annihilation attacks [91, 58, 92]. For example, pulse duration (1-2 ns) is insignificant in performing meaningful distance reduction, as discussed in the next section. If the pulse phase is unknown to the attacker, generating an inverted pulse to perform cancellation is considered difficult due to processing delay and the attacker's position with respect to legitimate devices.

2.4 Security Primitives for Secure Distance Measurement

So far, ToF based ranging systems are considered secure against distance reduction attacks if they adhere to the principles proposed by Clulow *et al.* [91]. There does not exist enough literature to enable security against distance enlargement attacks.

Principle 1." Use a communication medium with propagation speed close to physical limit through space-time, i.e., the speed of light in vacuum." - This principle is required to prevent relay attacks on the ToF based ranging systems.

Principle 2. "Short symbols (preferably one pulse per symbol) are necessary for secure ranging." - This restriction is applied due to the threat of ED/LC attack.

Principle 3. "Rapid pulse exchange is necessary for secure ranging." - Following this principle is necessary to prevent ED/LC attack on multi-bit systems.

Principle 4. "Special bit-error tolerant protocols are required at the logical layer." - The long-distance or NLoS conditions are not favorable for the

short symbol structure. Therefore, logical layer protocols should be capable of handling bit errors.

These principles restricted the choice of communication medium, communication format to single bit messages, symbol length to short, and protocols to error-tolerant versions. These restrictions increase hardware complexity, introduce challenges in implementing secure distance bounding and limit the distance we could measure using these implementations. These might be reasons that none of the commercially available ranging systems adhere to these principles [38, 93, 37]. Furthermore, following these principles does not guarantee security against distance enlargement attacks.

Message Time of Arrival Codes (MTACs) has been introduced to capture the physical layer aspects not captured by distance bounding protocols and relax secure ranging principles mentioned above [94]. The idea is to use MTACs to construct a message to symbol encoding that preserves the legitimate signal ToA against an adversary that tries to "shift" the signal in time, *i.e.,* aim to create the impression of a different arrival time. Fundamentally, the adversaries can aim to produce the code earlier than its legitimate appearance (advancement) or erase any evidence of a signal, thus opening the possibility for a late imitation (delay). These codes consist of a tuple of probabilistic polynomial-time algorithms as follows.

Key-generation: This algorithm is used to generate a key that the verifier and the prover use for the ranging. We consider that the key is freshly generated and contains sufficient entropy. In this thesis, we focus on code generation and verification algorithms, assuming that the devices performing ranging share a large amount of ideal randomness.

Code-generation: This algorithm converts a message (*e.g.,* nonce n_{VE} and n_{PR}) into a code of real-valued vector $S = (s_1, s_2, .., s_n)$ - the signal that is transmitted at the physical layer. Each value in the code represents a sample, and sample duration depends on the system's sampling rate. The idea is that like bits can be encrypted with a shared key, the shape of a signal can also be hidden, *e.g.,* by masking it with a random fast-changing sequence, therefore preventing ED/LC and signal annihilation attacks. This code aims that for a sufficiently wideband system, the ToA manipulation should be restricted by the sample duration (*e.g.,* pulse duration of $\sim 1-2ns$ in UWB ranging systems), which is insignificant in terms of distance manipulation (less than a meter).

Verification: Since received signal is affected by multipath, noise, interference, and attack signal, the reliability of code depends on the verification algorithm's ability to distinguish noise, legitimate signal, and attack signal.

Attacker Model: As considered in the threat model above, the attacker is aware of code-generation and verification algorithms used by the system. Based on the system's design, messages (data bits) can be known or hidden from the adversary; they can observe message to code mapping for the messages of their choice, but they cannot predict the code a device is using during a ranging instance. However, they can acquire knowledge of the partial code, the part of the code already being transmitted by the legitimate transmitter. When a legitimate entity is transmitting a sample s_i of the code, the attacker has access to $s_{i-\delta}$ legitimate samples. Delay $\delta = 1$ is considered to provide maximum advantage to the attacker. This observation delay includes propagation delay due to the attacker's location and the processing time of the sample. For a sufficiently wideband system, such as UWB, the observation delay according to this requirement would be bounded by a few ns. An attacker can use these samples to predict remaining samples to either advance their arrival time or annihilate them and, therefore, succeed in performing distance reduction and enlargement attacks. Informally speaking, the ranging system is considered secure if the probability of winning for an efficient adversary with these capabilities is small.

2.5 Summary

In this chapter, we discussed different approaches to perform distance measurement and outlined a threat model to evaluate their security. We show that ranging systems, including ToF based ranging systems, are vulnerable to distance manipulation attacks; the perceived distance can be enlarged or shortened by manipulating the legitimate signal. An attacker can mount attacks at the logical or physical layer. We can prevent logical layer attacks by implementing distance bounding protocols, but these protocols fall short if an attacker is capable of performing physical layer attacks. We showed that systems using properties of the received signal for distance measurement have fundamental limitations, and they cannot be trusted to provide secure ranging. ToF based ranging systems can provide security against distance reduction attacks at the cost of limiting their performance. On the other hand, there is not enough research to detect

distance enlargement attacks. In addition to that, we discussed security primitives that should be considered when designing a secure-ranging system to prevent distance reduction and enlargement attacks. The ranging systems should be analyzed under MTAC attacker model to ascertain their security.

Part I

UWB Ranging

Chapter 3
Security Analysis of UWB Ranging Systems

In recent years we have witnessed the widespread deployment of UWB ranging systems. UWB chips are now embedded in smartphones—Apple iPhones are using UWB for spatial awareness [68], Samsung's latest phone aims to use UWB ranging as a *digital key* to unlock the front door of the house [69], several car manufacturers, including Volkswagen and Mercedes, are using UWB chips to protect their Passive Keyless Entry and Start Systems (PKES) against relay attacks [43], and many companies have announced the use of UWB ranging for contact tracing [95, 96]. The use of UWB ranging systems in different industrial and home applications is only expected to grow.

Most of the recent UWB deployment follows IEEE 802.15.4a/f/z UWB ranging standards [97, 98, 99]. The IEEE 802.15.4z was in development for several years and was finalized in 2020. This standard enhanced the existing IEEE 802.15.4a and IEEE 802.15.4f standards with new integrity features, allowing more precise and secure ranging. 802.15.4z has standardized two modes of operation – Low Rate Pulse (LRP) and High Rate Pulse (HRP). The LRP mode has extended IEEE 802.15.4f with the distance bounding and distance commitment to enable secure ranging [99, 58] and this mode is currently deployed in automotive for PKES Systems [44], and available in Microchip ATA8352/8350 chips [100]. HRP, on the other hand, has proposed Secure Training Sequences (STS) for time-of-flight measurement. HRP chips are already deployed in Apple iPhones (U1 chips) and available in NXP Trimension SR150/SR040 chips [101]. The modes for UWB ranging differ in packet format, modulation scheme, pulse repetition frequency, and receiver design. We show that these configurations collectively define the security and performance tradeoffs of these systems.

This chapter analyzes the security of existing UWB ranging systems based on the IEEE 802.15.4f/a/z standards. We show that computing ToA using preamble is vulnerable to Cicada attack, and longer symbols allow the possibility of ED/LC attack [60, 59]. Therefore, we can not trust UWB ranging systems based on 802.15.4a and 802.15.4f (long and extended mode) to establish secure ranging. We show that the base mode of 802.15.4z/f provides a provably secure ranging system when used with distance bounding and distance commitment; the achievable security

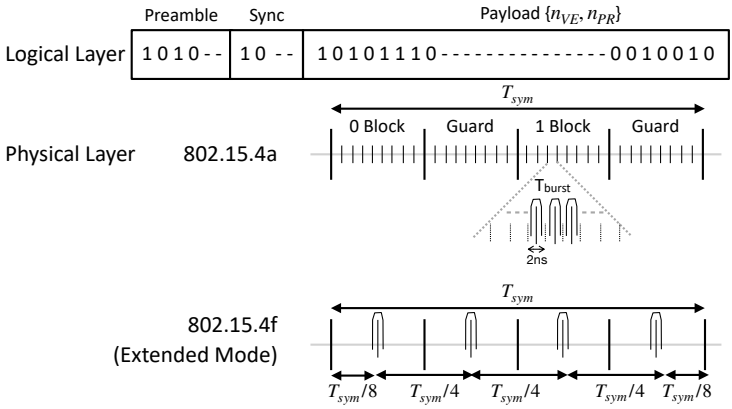


Figure 3.1: 802.15.4a and 802.15.4f propose different modulations for mapping a ranging packet to a physical signal. This illustration refers to the respective modes geared towards long distances.

depends on the attacker's ability to guess payload bits generated by the distance bounding protocols. However, extended and long-range modes of LRP are still vulnerable to distance manipulation attacks. We then explore the security and performance tradeoffs of the HRP mode. This analysis tells us that existing ranging systems cannot be trusted to enable secure ranging if performance is equally important.

The rest of the chapter is organized as follows. In Section 3.1, we review the most relevant concepts behind UWB ranging standards. In Section 3.2, we provide an overview of the distance reduction attacks possible on the UWB ranging systems, including UWB LRP and HRP. Section 3.3 discusses possible enlargement attacks on UWB ranging systems. We conclude our findings in Section 3.4.

3.1 UWB-IR

Prior to the standardization of UWB ranging in IEEE 802.15.4z, the UWB ranging systems were based on IEEE 802.15.4a and IEEE 802.15.4f standards. All these standards allow the use of 500 MHz-bandwidth channel located in a frequency range between approximately 3 GHz and 10 GHz. Transmit power is limited by FCC and ETSI regulations. The standards do not specify transmitter or receiver implementations. Nevertheless, they propose different modulation schemes with different

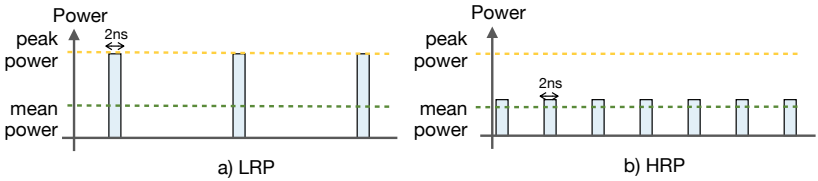


Figure 3.2: Transmit power of pulses in 802.15.4z LRP and HRP mode.

Pulse Repetition Frequencies (PRF) and the number of pulses in a symbol as shown in Figure 3.1. The motivation of different PRF stems from the fact that the device operates in different environments with widely varying delay spread. Therefore, the 802.15.4a device should support mandatory low (3.9 MHz) and high PRF (15.6 MHz) and adapt PRF based on the channel condition. 802.15.4f supports only low-PRF of 1-2 MHz which reduces location ambiguity and improves the performance of the non-coherent receiver in the high multipath environment.

The symbol length (T_{sym}) depends on the modulation scheme, the number of pulses in the symbol, and the PRF. The motivation of different PRF stems from the fact that the device operates in different environments with widely varying delay spread. Therefore, the 802.15.4a device should support mandatory low (3.9 MHz) and high PRF (15.6 MHz) and can adapt PRF based on the channel condition. 802.15.4a uses Burst Position Modulation (BPM) and Binary Phase Shift Keying (BPSK) to accommodate coherent and non-coherent receivers. 802.15.4f supports only low-PRF of 1-2 MHz which reduces location ambiguity and improves the performance in high multipath environment. 802.15.4f supports a base mode that encodes each bit in one pulse (on-off keying) as well as extended and long-range modes that encode each bit in multiple UWB pulses. 802.15.4f achieves lower complexity in terms of low power consumption and low cost using OOK modulation and non-coherent receiver design.

IEEE 802.15.4z standard, finalized recently in 2020, aims to address physical layer attacks and introduces enhancements to improve the ranging capabilities of the UWB-IR, including precision, security, and MAC layer support. The standard specifies two modes of operation: Low Pulse Rate (LRP) and High Pulse Rate (HRP).

HRP vs LRP: As their names suggest, the modes have different PRF, which determines the spacing between pulses. In the HRP mode, there is a smaller spacing between pulses but, as a consequence, also a lower power per pulse

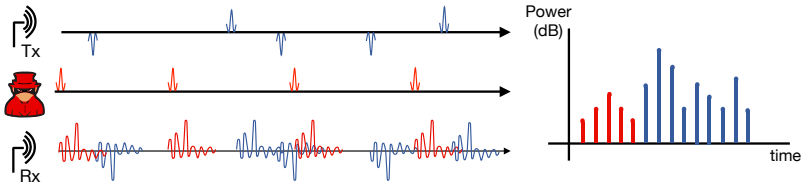


Figure 3.3: Cicada attack on UWB preamble.

compared to the LRP mode, in order to satisfy the power spectral density of $-41.3\ dBm/MHz$, as shown in Figure 3.2 [57]. While the channel noise affects both modes, pulses sent with the HRP mode suffer from inter-pulse interference, as the spacing between consecutive pulses is smaller than the delay spread of the channel. A single LPR pulse modulated with On-Off-Keying (OOK) or Binary Frequency Shift Keying (BFSK) can be used for early path detection. HRP, on the other hand, uses Secure Training Sequence (STS), a Binary Phase Shift Keying (BPSK) modulated sequence of pulses, and ToA estimation is done by accumulating samples over STS duration.

3.2 Distance Reduction Attacks on UWB Ranging Systems

UWB-IR ranging systems rely on time-of-flight measurement for distance estimation; they are therefore inherently secure against distance reduction by relay attacks. However, there exists the possibility of distance reduction by manipulating ToA estimation of the preamble (cicada attack) and the payload (ED/LC attack).

Cicada Attack: Poturalski *et al.* [59] showed ToA manipulation attacks on 802.15.4a by degrading the receiver's performance, as shown in Figure 3.3. The attacker transmits pulses with the same polarity at the uniform repetition period with the intention to inject a peak earlier than the legitimate first/early path. An attacker can perform a similar attack to manipulate ToA estimation on the 802.15.4f packet's preamble. We can prevent the ToA advancement by limiting the backsearch window. However, this degrades the system's performance in benign NLoS conditions; backsearch duration should be longer than the time difference between the early and strongest peak's arrival time.

Early Detect Late Commit Attack: Flury *et al.* [61, 60] showed the possibility

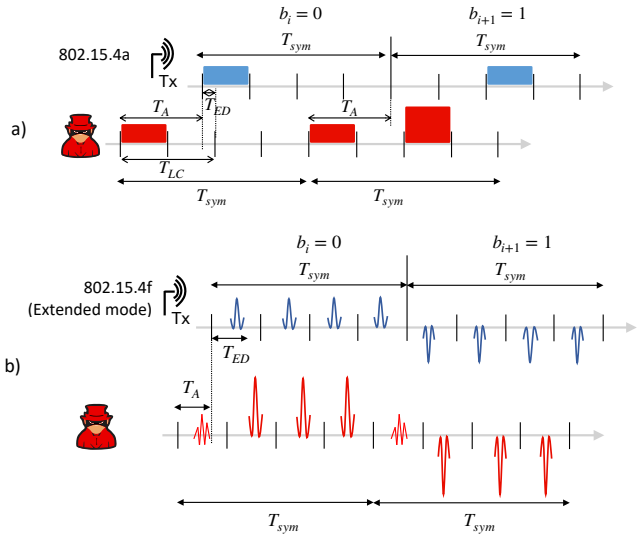


Figure 3.4: ED/LC attack on UWB 802.15.4a and 802.15.4f (extended mode) payload symbol

of ED/LC attack on BPM + BPSK modulation used in 802.15.4a, as shown in Figure 3.4a. For example, when 802.15.4a implementation is used with the non-coherent receiver, the receiver compares energy between block-0 and block-1 (as shown in figure 3.1) for data demodulation. To advance the symbol's arrival time, an attacker can commit the attack signal T_A ns earlier than the legitimate symbol transmission, where $T_A < T_{sym}/2$. After detecting block-0 of the legitimate symbols (T_{ED}), the attacker can make an informed decision to send pulses in block-1. Therefore, an attacker can control the output of the hypothesis test at the receiver.

Extended and long-range modes of 802.15.4f rely on multiple pulses per bit. Unfortunately, due to long symbol lengths and predictable symbol structures, these modes are also vulnerable to ED/LC attacks. An attacker can early detect the polarity of the legitimate pulse (as shown in Figure 3.4b) and choose polarities of the remaining pulses, such that they produce correct data at the receiver.

The only prevention against ED/LC attack is to use short symbols, where a single pulse represents one bit of information. A short symbol given by a single narrow pulse ($1-2$ *ns*) is considered secure against an ED/LC attack. Tippenhauer *et al.* [58] designed a system to process short symbols.

To minimize symbol length, they allocate energy within a time frame as short as feasible. This leaves little room for an attacker to shorten the time measured. Existing proposals against ED/LC attacks provide the choice between longer symbols (longer distance) and security. Later in Chapter 4, we propose an approach to enable secure raging on the extended mode of IEEE 802.15.4f.

3.2.1 Security Analysis of UWB 802.15.4z HRP

The HRP mode of IEEE 802.15.4z has implemented Secure Training Sequence (STS) to enable secure ranging. However, there does not exist any open source analysis. Along with the STS sequence, the ranging packets can also accommodate a preamble and payload, as shown in Figure 3.5. The standard does not define the use of preamble and payload for ToA estimation. Using those parts of the packet for distance estimation would not increase the security of distance estimation. The preamble is predictable, and thus an adversary can send it in advance. The payload is BPM+BPSK modulated, as in the IEEE 802.15.4a, allowing ED/LC attack.

Secure Training Sequence (Code Generation) is a Binary Phase Shift Keying (BPSK) modulated sequence of pulses generated from a pseudorandom bit generator. A bit of value zero produces a positive, and bit of value one produces a negative polarity (phase) pulse. These pulses are sent with the PRF of 124.8 MHz. A ranging packet can have up to two STS sequences, and each STS sequence can be divided into two segments of at least 4096 pulses each. The segments are encapsulated by silent intervals/gaps of 512 chip ($\approx 1\ \mu s$) duration. The receiver calculates the ToA by correlating the received signal with a local STS template that has been generated using the same seed as the sender's STS. Thus, the receiver can use each STS segment to estimate and validate the integrity of the arrival time. However, the standard does not specify the receiver design.

UWB HRP Receiver Design (Verification) The receiver design mentioned by the standard [99, 102] suggests computing the Channel Impulse Response (CIR) using STS by correlating the incoming signal with the locally generated template. After the correlation operation, the receiver needs to find the highest correlation peak and then identify a peak that indicates the first occurrence of the STS during a backsearch window. There are several aspects and implementation choices that determine whether the ranging operation is resilient to external interference.

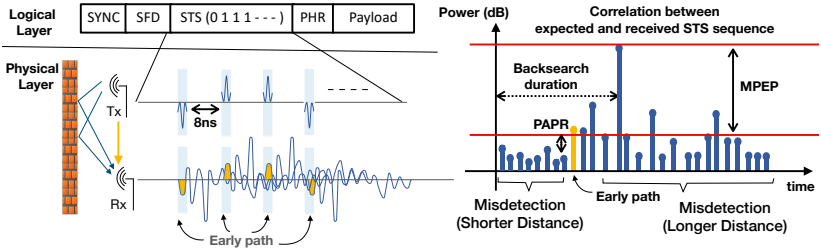


Figure 3.5: The HRP uses STS to enable secure distance measurement. A random bit sequence is modulated into pulses. Bit of value one and zero are represented by different polarities (phase). Pulses observe inter-pulse interference due to high PRF.

Physical phenomena, such as multipath fading, require a robust and fault-tolerant time-of-flight estimation technique not to render the system useless (e.g., NLoS). As shown in Figure 3.5, we can use Peak to Average Power Ratio (PAPR) and Maximum Peak to Early Peak ratio (MPEP) to differentiate early peak from noise and multipath. In such a receiver design, the value of backsearch window duration, PAPR, and MPEP should be chosen to minimize misdetection. Misdetection can indicate distance shortening if the peak used for distance estimation has arrived earlier than the early path. It can also mean distance enlargement when a peak arriving after the early path is used for distance measurement.

Distance Reduction Attack The STS is included in the HRP mode to enable secure ranging and prevent ED/LC and Cicada attack [102, 103]. In the absence of multipath and receiver noise, HRP with STS can implement a secure ranging system. In such a scenario, the receiver might decode most of the individual pulses of the STS sequence and require a high correlation of the received and template STS. However, since an adversary cannot predict the pseudo-randomly generated sequence, it will not generate a high enough correlation peak that satisfies the checks applied at the receiver. However, this scenario is unlikely in the presence of the multipath; the highest correlation peak is not always caused by the signal that arrived along the direct path [104]. The receiver, therefore, needs to search for the peak corresponding to the direct path in the backsearch window.

An important observation is that, in order to manipulate the arrival time estimation, an adversary does not need to inject or manipulate the highest correlation peak. This allows for Cicada-like attack to succeed in the

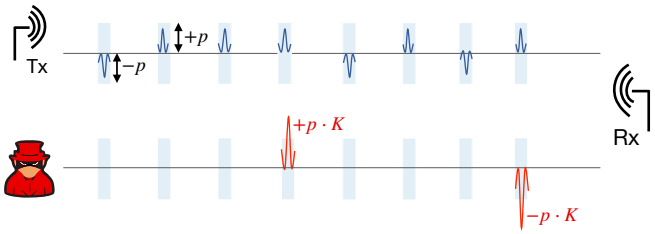


Figure 3.6: Example of *Cicada++ Attack*. The adversary is transmitting random polarity pulses with lower PRF, and higher transmit power than the legitimate pulses.

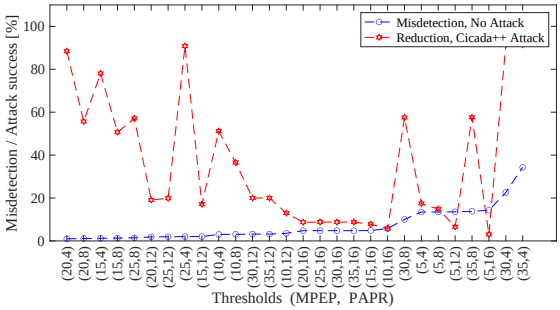


Figure 3.7: The different choices of thresholds (MPEP, PAPR) can provide either a secure or performant system. In scenarios where chances of attack success are low (*e.g.,* MPEP $= 5\ dB$), the system is more likely to provide inaccurate distance measurement.

distance reduction attack. Figure 3.6 shows a variation of the cicada attack, known as cicada++ attack [105]. The attacker injects uniformly spaced pulses with lower PRF and higher transmit power than the legitimate STS sequence. The receiver, therefore, receives superposition of the legitimate signal and the attacker's signal. Since large parts of the legitimate STS arriving at the receiver is unmodified (i.e., whenever legitimate transmission does not coincide with an attack pulse), the receiver can still successfully correlate the transmission with the local template of the STS and observe a high correlation peak. On the other hand, the attacker's signal increases the power of the side peaks. It is harder for the receiver to differentiate if such earlier peaks (satisfying PAPR and MPEP thresholds) are generated in

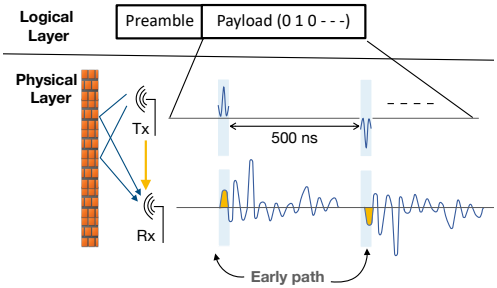


Figure 3.8: The LRP uses distance bounding and distance commitment to enable secure ranging. Pulses are not affected by the inter-pulse interference, and receiver can resolve polarity of each pulse in the short range LoS conditions.

a non-adversarial (e.g., NLOS) setting or caused by a superimposed attack signal.

As shown in Figure 3.7, the cicada++ attack is effective against a varied range of receiver parameters and varying channel conditions. For all receiver settings where misdetection is low ($< 1.5\%$), the attack success rate is at least 50% for backsearch window duration of 128 *ns*, computed over randomly chosen channel conditions [106]. Therefore, HRP mode can either achieve a reliable or secure system using STS and the given receiver design, but no receiver configuration can fulfill both requirements. The distance measurement is classified as misdetection or attack when inaccuracy in the measured distance is more than 7 *ns* (2.1 *m*). These results suggest that HRP cannot be considered a secure MTAC, as reliable verification is not possible using STS with the given receiver design.

3.2.2 Security Analysis of UWB 802.15.4z LRP

LRP (Code Generation) Figure 3.8 shows the packet format used by the LRP mode in IEEE 802.14.4z. The packet contains a preamble (synchronization header and start-of-frame delimiter) and a payload. The payload is generated cryptographically using distance bounding protocols. The LRP mode has adopted all modes (base, extended, and long) of the IEEE 802.15.4f standard. The extended and long-range modes use multiple pulses to represent one bit of information, and the base mode uses a single pulse to represent one bit of information. The symbols in LRP

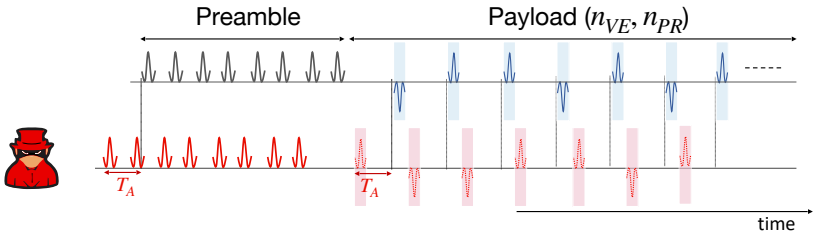


Figure 3.9: Due to the use of distance commitment in LRP mode, if an attacker advances the arrival time of the preamble, the attacker also needs to advance the payload's arrival time. When using LRP base mode, the probability of advancing the arrival time of payload symbols is equivalent to predicting data bits generated by distance bounding protocol.

can be modulated with BFSK, as compared to only OOK in 802.15.4f, and pulses can be transmitted at the PRF of 1 MHz, 2 MHz, or 4 MHz.

UWB LRP Receiver Design (Verification) Since LRP uses OOK and BFSK modulation, a non-coherent receiver is sufficient for the ToA estimation and data detection. The LRP mode also mandates distance commitment for ToA estimation and verification [58]. The receiver applies leading-edge detection algorithm on the preamble (synchronization header) for ToA estimation. This ToA estimate is used to determine when to expect samples for the payload. As shown in Figure 3.8, the early/direct path of the pulses is not affected by multipath components; the transmission time between two pulses is longer than the delay spread of the channel. If the signal arriving through direct has sufficient energy, the receiver can easily compute ToA and validate it by recovering correct data. The distance measurement is discarded if the data is incorrect. These systems can tolerate some bit errors to increase performance under NLoS and long-distance ranging scenarios.

Distance Reduction Attack In order to perform the distance reduction attack, an attacker needs to advance the arrival time of preamble and payload. The attacker can always send a preamble earlier than the transmission of the legitimate packet, as it is a known sequence of pulses. The arrival time of the preamble is binding to the arrival time of the payload pulses. Therefore, if a receiver computes an earlier ToA, it also searches for the payload earlier, as shown in Figure 3.9. If LRP is used with the extended or long mode, it is vulnerable to the ED/LC attack.

However, for the base mode of LRP, irrespective of OOK or BFSK modulation, the attack success depends on guessing the payload bits generated using distance bounding protocols (*i.e.,* n_{VE} and n_{PR}). Therefore, we can consider that LRP's base mode is secure, and the security level depends on the number of bits transmitted and bit errors allowed by the distance bounding protocol. For example, under the assumption of ideal randomness and an unbounded adversary (observation delay $\delta = 1$ according to MTAC definition), we achieve 32 bits of security against distance advancement attack by transmitting 116 bits while tolerating up to 20% bit errors. Therefore, we can consider that the LRP base mode constructs a secure MTAC.

3.3 Distance Enlargement Attacks on UWB Ranging Systems

In contrast to reduction attacks, an attacker can enlarge the measured distance by delaying the signal's arrival time at the receiver. In order to achieve successful distance enlargement, the receiver should discard legitimate signal as noise and use attack signal for ToA estimation and payload detection. An attacker can prevent legitimate payload detection by increasing the bit error by adding noise in the channel or canceling some of the pulses. Given that the attack signal is a replica of the legitimate signal and arrives at the receiver with the higher power, the receiver decodes correct data for the delayed (and replayed) attack signal.

To manipulate ToA, an attacker can simply replay the signal with the higher power as shown in Figure 3.10a and Figure 3.10b. In the replay attack, the attacker can use a random value for the delay T_D. However, to achieve overshadowing, the attack pulses should fall over the legitimate pulses, *i.e.,* $T_D = n * T_s$, where n is a positive integer, and T_s is the spacing between two consecutive pulses depending on the PRF. However, there exists the possibility of early path detection during backsearch [87]. Compagno *et al.* provide a probabilistic model to predict the outcome of overshadowing attack on 802.15.4a symbols and showed that the attack signal behaves like high multipath signal [107].

In order to prevent the detection of the early path during backsearch, an attacker can perform legitimate signal annihilation as shown in Figure 3.10c. If the phase of the pulses is predictable, an adversary can transmit pulses with the reciprocal phase to perform signal cancellation, therefore, controlling ToA estimation. In scenarios where a legitimate transmitter and receiver are not able to communicate (*e.g.,* signal blocked

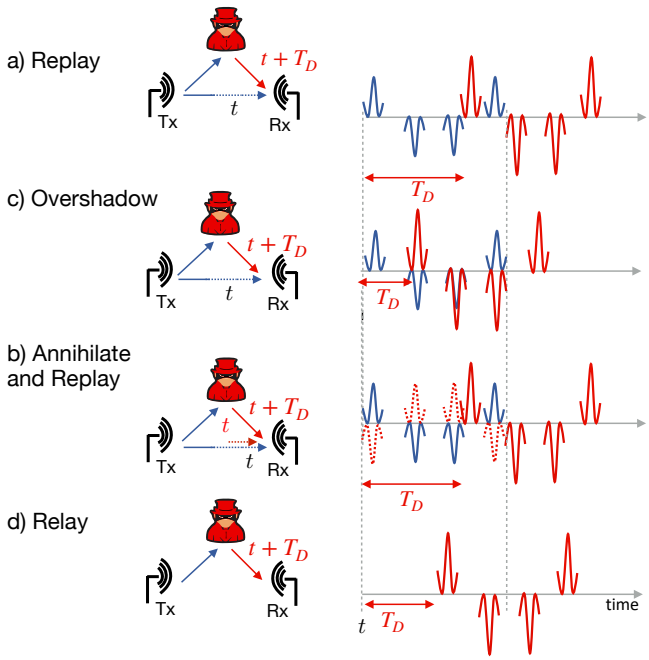


Figure 3.10: Different distance enlargement attack scenarios on UWB. Blue and red colors represent authentic and adversary signals, respectively. Dotted red represents adversarial signal-annihilation attempts..

due to NLoS), an attacker can simply relay the legitimate signal to perform distance enlargement attack as shown in Figure 3.10d. We can apply these attacks on the LRP (preamble) and HRP (STS) to prevent early path detection during backsearch.

Tippenhauer *et al.* [92] explored a theoretical approach to detect adversarial signal annihilation using a single pulse-per-symbol. They found that modulation with a 2 *ns* sample duration, *i.e.,* mostly equivalent to pulse width, might help detect signal annihilation. This limits the ranging technique to short distances. Nevertheless, it showed the possibility of enlargement attack detection at the physical layer if we can prevent attackers from performing signal annihilation, and traces of the legitimate signal arrive at the receiver. For example, STS would prevent pulse cancellation as the phase of pulses is unpredictable for the attacker [103]. However, an attacker may succeed by overshadowing STS

and elevating average noise to prevent legitimate peak detection. We explore an approach to detect distance enlargement attack further in Chapter 5.

3.4 Conclusion

In this chapter, we provided an overview of the distance manipulation attacks on different modes proposed in the 802.15.4a/f/z standards. The modulations presented in 802.15.4a and 802.15.4f are vulnerable to distance reduction by cicada and ED/LC attacks, except the base mode of 802.15.4f that uses a single pulse to represent one bit of information. 802.15.4z standard has enhanced 802.15.4a and 802.15.4f with new security constructs and integrity checks. The use of distance commitment in LRP mode has relaxed the requirement of rapid-bit exchange. There still exists the possibility of the ED/LC attack on extended and long-range modes. Therefore, the UWB LRP system needs to choose between security and performance (performance under long-range and NLoS conditions). On the other hand, distance estimation using HRP is purely based on STS, security hinges on leading-edge detection. The analysis of HRP revealed that a sequence of random phase pulses is insufficient to design a secure ranging system. This analysis shows that we need to consider physical layer design from the perspective of both transmitter and receiver.

Chapter 4
UWB-PR: Distance Reduction Attack Prevention in UWB

Attempts have been made to design secure UWB ranging systems, for example, LRP and HRP mode of UWB IEEE 802.15.4z. However, randomizing polarity of pulses to achieve secure ranging has proven to be insufficient in achieving secure ranging, as shown by the analysis of the HRP mode in the last chapter. On the other hand, LRP base mode, in combination with distance bounding and distance commitment, realizes a secure ranging system [58, 91]. Instantaneous transmit power in any practical UWB system faces constraints originating from both regulatory bodies and hardware integration concerns; the pulse's energy is limited, therefore limiting the range. In addition, standards imposed limitations on the amount of energy that can be placed in a short time frame, further rendering single pulse systems inadequate for NLoS and long-distance communication. Therefore, for distance measurement under such conditions, we need longer symbols with multiple pulses per bit. However, increasing the symbol length is considered vulnerable to ED/LC attack [91], where an attacker predicts the internal structure of the symbol to advance its arrival time. Due to the possibility of these attacks, existing systems can be either secure or performant regarding their range and resilience to NLoS conditions but not both.

In this work, we address this problem and propose *UWB with Pulse Reordering* (UWB-PR), the first modulation scheme that secures distance measurement between two mutually trusted devices against all physical-layer distance reduction attacks and enables long-range distance measurements. UWB-PR uses pulse reordering and cryptographic pulse blinding to prevent physical-layer attacks, allowing UWB systems to securely scale to longer symbols (multiple pulses per bit) for long-distance and performance. UWB-PR is compatible with 802.15.4 UWB as well as FCC and ETSI regulations. This can be considered as an extension of the IEEE 802.15.4f or 802.15.4z LRP extended mode.

UWB-PR provides quantifiable probabilistic security guarantees without making any assumptions regarding channel conditions or attacker positions. Finally, UWB-PR combines data transfer and distance measurement, and allows secure distance measurement on multi-bit nonces. It is therefore

compatible with the majority of existing distance bounding protocols [19, 23].

We analyze the security of UWB-PR analytically and through simulations. We show that, at any symbol length, UWB-PR allows to extract security guarantees from longer nonces n_{VE} and n_{PR} in two ways. First, more bits interleaved by means of the reordering operation lower an attacker's chances of guessing any individual bit. Second, longer overall nonces decrease the chances of an attacker guessing the entire sequence n_{VE} or n_{PR}, as all bits have to be guessed correctly. We further implemented UWB-PR within a UWB transceiver and show that it achieves a range of 93m with a precision of 10cm.

The remainder of this chapter is organized as follows. Section 4.1 establishes that longer symbols cannot be avoided if we want to achieve performant UWB ranging systems. We introduce our approach UWB-PR in Section 4.2 and analyze its security in Section 4.3. Section 4.4 discusses the performance and security of our 802.15.4f-compatible proposal in relation to the 802.15.4a standard as well as limitations of our approach. We revisit ranging principles for designing secure ranging systems in Section 4.5. Section 4.6 concludes.

4.1 Design Space

4.1.1 Single-Pulse vs. Multi-Pulse Systems

Because UWB systems operate over wide segments of licensed spectrum, they have to be compliant with stringent regulatory constraints. Firstly, the power spectral density cannot exceed $-41.3\ dBm/MHz$, averaged over a time interval of 1ms. Secondly, the power measured in a 50 MHz-bandwidth around the peak frequency is limited to 0 dBm.

Long symbols are associated with unfavorable outcomes in ED/LC attacks. Therefore, a reasonable assumption might be that a system aiming primarily for security and long distance ranging will first try to maximize the power per pulse and then the PRF to guarantee the highest possible energy per symbol while keeping the symbol as short as possible. Optimally, such a system would hence exactly meet both constraints. Maxing out the average constraint can only be done for certain PRFs, however. Specifically, all PRFs below 187.5 kHz are less than optimal due to the power per pulse saturating under the peak power constraint [108].

Consequently, a single pulse per bit sent at a PRF of 187.5 kHz could theoretically be considered optimal in terms of security and performance. In practice, there exist legitimate incentives for higher PRFs and also increased

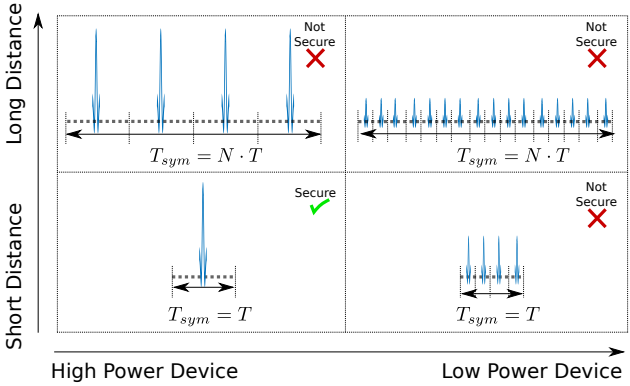


Figure 4.1: Two independent causes are driving the need for more pulses per symbol: Low instantaneous power and high performance in terms of energy per symbol, both under compliance with regulatory constraints. The higher energy per symbol is needed for the longer distance and NLoS measurements. However, longer and deterministic symbol structure make the system vulnerable to ED/LC attack.

numbers of pulses per bit, however. Data rates exceeding 187.5 $kbps$ can only be offered at higher PRFs since the bit rate cannot exceed the pulse rate in the burst position modulation (BPM) or on-off keying (OOK), the modulations used by 802.15.4a and 802.15.4f. Moreover, the instantaneous power can be a serious limitation imposed by the hardware, especially at high integration densities. Likely to accommodate for the latter, 802.15.4a, for instance, offers a range of different configurations, each with similar energy per symbol but varying PRFs and energy levels per pulse. This underscores the practical necessity of spreading out energy across pulses, even if regulations might not require it.

Given a certain PRF, increased performance and distance can always be achieved by increasing the symbol length. This fact gets reflected well in the extended mode of 802.15.4f, where a symbol consists of four pulses compared to only one pulse in the base mode. However, the PRF remains unchanged (and in particular, uniform).[1] As a consequence, this approach allows to achieve virtually arbitrary symbol energy, without violating regulatory and other power constraints, by constructing longer symbols.[2]

[1] Because the (local) PRF does not depend on the symbol duration here.
[2] Assuming that the oscillator drift remains reasonably bounded.

However, without securing the modulation, what essentially constitutes repetition coding is still highly vulnerable to ED/LC attacks. This is the problem addressed in UWB-PR.

We conclude that (i) irrespective of the PRF, longer symbols and more pulses per symbol reliably provide higher distances, and (ii) maxing out pulse power according to regulations might not be viable due to hardware constraints. This means that, for meaningful distances, a practical, highly integrated system will likely use multi-pulse symbols (and therefore be vulnerable to ED/LC attacks on the symbol level). These considerations are summarized in Figure 4.1.

4.1.2 Physical-Layer Cryptographic Operations

Multi-pulse UWB systems need to be secured against physical-layer attacks on ToF measurement by means of dedicated physical-layer cryptographic operations. Encrypting the data bits exchanged as part of distance-bounding protocols is not sufficient. An ED/LC attacker can exploit redundant, multi-pulse signal structures despite knowing nothing about the data being exchanged.

On the other hand, individual UWB pulses are too short for a meaningful ED/LC attack, as the theoretically achievable reduction would be less than 1 m. Therefore, the focus of cryptographic operations is to make it impossible for an attacker to exploit the redundant encoding of information bits in multiple consecutive pulses. This is equivalent to hiding the way a receiver generates information bits from a train of UWB pulses. Physical-layer cryptographic operations are not related to the data transmitted on the logical level (i.e., the bits). In the same sense that bit-level cryptography does not protect against physical-layer ED/LC attack, bit-level data is not affected by the specific secrets used for physical-layer encryption. These operations, therefore, add an additional layer of security, specifically to protect against those attacks. Physical-layer cryptographic operations randomize the pulse sequence, given some bit-sequence to be transmitted.

Irrespective of how the information is encoded in the pulses (OOK, FSK, PSK), we can model each pulse as having two polarities. We argue that physical-layer cryptographic operations can be concerned with (i) XORing the pulse polarities with a random sequence[3] and (ii) hiding the timing of pulses belonging to a given bit. UWB-PR relies on the first and employs the latter mechanism by reordering[4] the pulses of consecutive bits.

[3] freshly generated for each transmission

[4] also, freshly generated for each transmission

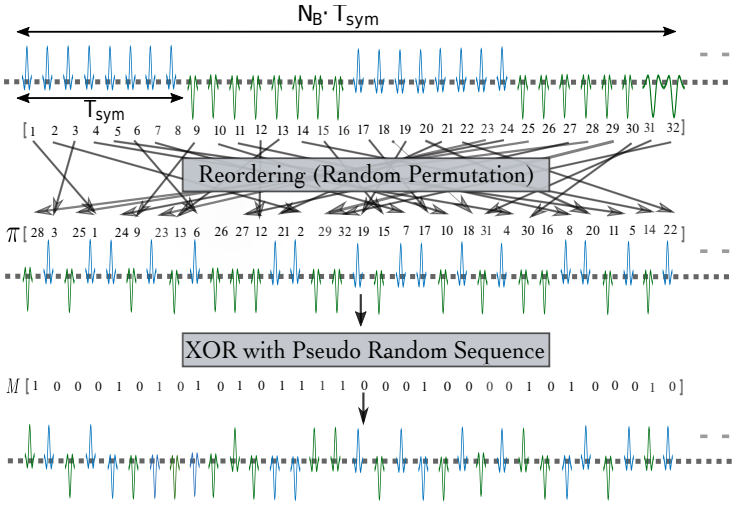


Figure 4.2: UWB-PR randomly reorders UWB pulses associated with N_B consecutive bits and cryptographically blinds their polarities before transmission.

4.2 UWB with Pulse Reordering

UWB-PR is a new modulation technique that enhances the extended mode of 802.15.4f with cryptographic operations at pulse level to prevent all physical-layer attacks on ranging, including ED/LC, while retaining the range and performance of the extended mode. To the best of our knowledge, UWB-PR is the first modulation to prevent ED/LC attacks independently of communication range offered.

The main intuition behind UWB-PR is provided in Figure 4.2. UWB-PR randomly reorders the UWB pulses that are associated with each bit and cryptographically blinds their polarity before transmission. Since a successful ED/LC attack is based on the attacker knowing the shape of the symbol as well as when the symbol starts and ends, pulse reordering prevents this attack by blinding the pulse polarity, through XOR with a preshared sequence, and by reordering pulses such that the attacker does not know which pulse belongs to which bit (i.e., where each bit starts/ends).

In ED/LC, the attacker implicitly relies on deterministic mappings between symbol positions and bits. In both 802.15.4a and 802.15.4f, this assumption is justified, since symbols consist of consecutive UWB pulses.

UWB-PR introduces uncertainty for an ED/LC attacker in both assessing past symbols and deciding when to interfere in the future (in order to affect a certain bit). While ED/LC attacks require an attacker being able to effectively decouple timing from cryptographic uncertainty, the reordering of UWB-PR cryptographically couples the random bits and pulse timings. As a consequence, an attacker has to guess correctly both the symbol values and symbol timings in order to guess a bit and is uncertain about the progress of the attack at any time.

Distance Measurement with UWB-PR: As in the LRP mode of 802.15.4z, UWB-PR relies on the distance commitment for the ToA measurement and verification [58]. While an attacker can trivially send the preamble early in an attempt to reduce the distance, he still has to guess subsequent protected symbols to be successful. The preamble does not contain any information about the nonces n_{VE} and n_{PR}. The timing of the preamble simply tells the receiver when to expect this secret information. Correct detection and verification then depend on this time offset being consistent with the actual timing of the UWB-PR pulses constituting n_{VE} and n_{PR}. The timing of the preamble is therefore binding. If the preamble is sent early, each subsequent pulse will be expected earlier by the receiver, essentially forcing an attacker to guess each pulse for successful verification. If the preamble alone is sent early (*i.e.,* by manipulating ToA estimation), the receiver will detect the inconsistency in the timing of the preamble and the secret payload or might not be able to recover the data at all, dismissing the claim in both cases.

4.2.1 Tx/Rx Chain (Code Generation and Verification)

Previous considerations make OOK, BFSK, and BPSK modulation as used in 802.15.4f/z reasonable choices for our system. In the following, we introduce major steps involved in the transmission and reception of a bit sequence with UWB-PR. This involves the encoding, which accommodates our main security features, as well as the continuous time signal representation and subsequent decoding.

Pulse Reordering As part of the encoding, we introduce a reordering of pulses that interleaves symbols of multiple consecutive bits. Consider first a deterministic encoding with N_P UWB pulses per bit. The reordering function R reorders the pulses of N_B consecutive bits as defined by a permutation π. π specifies the mapping between pulse positions before and after reordering. Π denotes the set of all possible reorderings. There are $|\Pi| = (N_P \cdot N_B)!/(N_P)^{N_B}$ ways to assign the pulses to bits, all equally

probable from the attacker's point of view. We design the system to choose a fresh, random reordering $\pi \in \Pi$ for each frame. This secret is assumed to be shared between verifier and prover before the ranging phase. The reordering function subject to some permutation is defined as

$$R(P, \pi) = (p_{\pi(0)}, ..., p_{\pi(N_P \cdot N_B - 1)}).$$

The reordered pulse sequence can in general be defined as

$$\hat{P} = R(P, \pi),\ \pi \overset{UAR}{\leftarrow} \Pi.$$

The choice of π being a secret shared by transmitter and receiver, an attacker has no knowledge that allows to link pulse positions to bits. From an attacker's point of view, all $|\Pi|$ reorderings are equally probable.

Pulse Blinding In addition to randomizing the pulse positions, we suggest to XOR the resulting sequence with a random bitmask M. We define the UWB-PR pulse sequence as the XOR of the reordered pulse sequence and a random bitmask:

$$\tilde{P} = \hat{P} \oplus M,\ M \overset{UAR}{\leftarrow} \mathcal{M}$$

The idea behind this is to guarantee high entropy in the resulting pulse sequence, irrespective of the choice of codes and bit sequences n_{VE} or n_{PR} at higher protocol layers. Again, we assume that M is chosen randomly for each exchange and shared between prover and verifier before the ranging phase.

Modulation In OOK, a binary sequence is encoded as a pulse either being present or absent at a known time. We consider regularly spaced pulse positions with period T_P. Under these assumptions, the transmit signal for a pulse sequence $\tilde{P}^{(b_1,...,b_{N_B})}$ of N_B interleaved bits consisting of N_p pulses each can be written as

$$s(t) = \sum_{k=0}^{N_B \cdot N_P - 1} \tilde{P}^{(b_1,...,b_{N_B})}[k] g(t - kT_P),$$

for a UWB base pulse g.

Demodulation The receiver optimally collects the energy at time kT_P by applying a matched filter $h = g(-t)$ as

$$y[k] = (s * h)(kT_P) = \|g\|^2 \tilde{P}^{(b_1,\ldots,b_{N_B})}[k],$$

where $*$ denotes the convolution operation. The receiver can construct the energy profiles for the bit-0 hypothesis

$$\tilde{P}_{H_0^k} = R((\ldots \| \underbrace{P^0}_{k\text{-th bit}} \| \ldots), \pi) \oplus M,$$

and the bit-1 hypothesis as

$$\tilde{P}_{H_1^k} = R((\ldots \| \underbrace{P^1}_{k\text{-th bit}} \| \ldots), \pi) \oplus M,$$

by applying the same randomness π and M for reordering and cryptographic blinding as on the tranmsit side.

The sufficient statistics for the bit-wise hypothesis can be obtained by correlating the received energy with the expected energy profiles for each hypothesis:

$$\sigma^k = \sigma_1^k - \sigma_0^k = \langle y, \tilde{P}_{H_1^k} \rangle - \langle y, \tilde{P}_{H_0^k} \rangle$$

Because the codes are orthogonal and of equal parity, and neglecting all channel nonidealities, the ideal statistic at the receiver evaluates to

$$\sigma^k = \begin{cases} \|g\|^2 N_P N_B/2, & \text{if } b_k = 1 \\ -\|g\|^2 N_P N_B/2, & \text{if } b_k = 0 \end{cases},$$

suggesting optimal detection of the k-th bit as

$$\hat{b}_k = \text{sign}(\sigma^k).$$

4.2.2 Proof-of-concept implementation

We evaluated UWB-PR in a prototype system transmitting BFSK UWB pulses at a system bandwidth of 500MHz. The pulses are sent at a peak pulse repetition frequency of 4MHz, i.e., with a spacing of 250ns. In terms of the regulatory transmission power constraints, this places UWB-PR in the regime dominated by the average constraint of -41.3dBm/MHz[5] [108].

The link budget of the resulting system depends on the number of pulses per symbol. Our implementation provides us with an equivalent

[5]This corresponds to -14.3dBm over the entire system bandwidth.

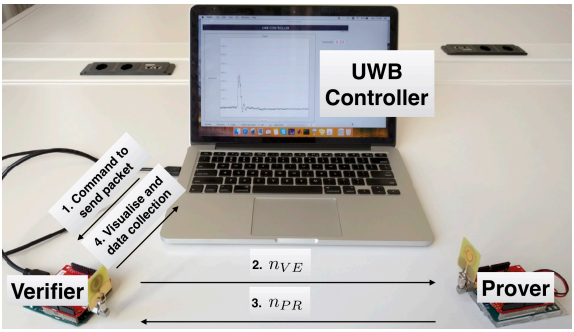


Figure 4.3: Illustration of our experimental setup. Actual measurements were obtained over a LoS channel for varying distances.

link budget[6] of about 79dB if it relies on a single pulse per bit. Within this margin, it can tolerate additional losses due to distance and shadowing. For instance, this configuration would allow operations up to distances of approximately 32m under LoS conditions. Robustness of signal transmission and, in turn, the maximum operating range can be further improved by increasing the number of pulses per bit.

For the experimental evaluation, we relied on 16 pulses per bit. This improves the link budget by 9dB to 88dB and results in an almost threefold maximum operating distance of 93m. There is no fundamental limitation to even longer symbols and corresponding distance improvements.

We evaluated the bit error rate for both a standard 802.15.4f-mode (i.e., without reordering) and a UWB-PR-mode relying on blinding and reordering over groups of four bits. Figure 4.3 shows our experimental setup. As the reordering can be configured in our prototypes, we were able to use the same hardware for both runs. The results for the bit error rate as presented in Figure 4.4 do not indicate any difference between legacy and UWB-PR systems. We also note that the ranging precision of 10cm (LoS) is not affected by the reordering operation since the distance measurement is executed on the preamble in both cases and is therefore independent of this operation.

[6]The maximum attenuation that still allows for successful ranging with likelihood > 0.01 per attempt.

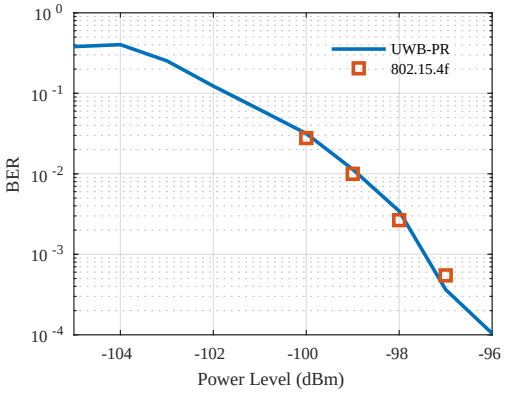


Figure 4.4: BER performance of UWB-PR as compared to 802.15.4f. Our experiments do not suggest any effect of the blinding and reordering operations on the bit error rate.

4.3 Security Analysis

UWB-PR is designed with the goal to provide performant ranging while guaranteeing quantifiable security against an external attacker. In particular, such an attacker should not succeed in reducing the distance between two mutually trusted parties, be it by means of a relay or by conducting any other physical-layer attack. A well-designed ToF distance bounding protocol with limited backsearch duration prevents distance reduction by cicada-like attacks. Since UWB-PR realizes on a distance commitment, the attacker needs to advance the arrival time of data bits if the attacker advances ToA estimation; the only remaining option for an attacker to reduce the distance measured is by advancing the signals representing the nonces (n_{VE} and n_{PR}), *i.e.,* by means of an ED/LC attack.

The attacker has to advance the arrival time of both preamble and payload data. The preamble is no secret, and the attacker can send it in advance. However, the payload is cryptographically generated. Upon locking on to the preamble, the receiver samples the payload pulses at specific times. The attack is only successful if the pulses sent by the attacker at these very instants yield the same correlation output at the receiver as the legitimate pulses.

The ED/LC attack involves predicting the part of the symbol, and conventional multi-pulse UWB systems have predictable symbol structures.

In UWB-PR, on the other hand, the pulses representing N_B bits are reordered, and their polarity is XORed with a secret sequence. An attacker does not know the pulse-to-bit mapping and the polarity of the pulses but can only try to *guess* this information. Guessing allows an attacker to send his pulse before observing the corresponding legitimate pulse. As we do not place any limit on the attacker's reception capabilities, we assume that he can resolve the legitimate signal at the pulse level. As a consequence, the attacker obtains feedback on the correctness of his pulse-guess immediately before transmitting the next pulse. The attacker has complete knowledge (power and polarity) of the legitimate $n-1$ pulses when the legitimate transmitter starts transmitting n^{th} pulse, which is equivalent to observation delay of $\delta = 1$ under the MTAC model. Moreover, we assume that the decision of the receiver only depends on the attacker signal, *i.e.,* the effect of the legitimate signal being negligible. This reflects a scenario where the legitimate prover is not in the vicinity of the verifier. An attacker guessing a polarity sequence P_A, transmitted with a sequence of power levels A, results for the k-th bit in the receiver statics.

$$\sigma_A^k = \|g\|^2 \langle AP_A, \tilde{P}^{(0,\ldots,b_k,0,\ldots)} \rangle.$$

The attack on the entire group of bits is successful if

$$\text{sign}(\sigma_A^k) = \text{sign}(\sigma^k), \ \forall k \in (0, \ldots, N_B - 1),$$

i.e. all bits decoded at the receiver based on the statistics produced by the attacker signal match the legitimate bits.

Without reordering and pulse blinding, the attacker knows the value of a bit after observing a small part of the symbol. As we explore in the next section, in UWB-PR, the guessing attacker's knowledge is only probabilistic.

4.3.1 Attacker Knowledge

Since the secret reordering and blinding sequences are chosen randomly for each transmission, an attacker cannot learn anything by observing multiple frames. Therefore, the evolution of an attacker's knowledge is confined to the specific pulse sequence within a single frame.

Attack Sequence S At each time t during an attack, the attacker knows all his past contributions in terms of transmission power and polarity as well as the true pulse polarities sent by the legitimate transmitter. Therefore, the attacker knows at each time all his past contributions to the bit-wise

decision statistics $\sigma_A^k, k \in \{1, ..., N_B\}$, at the receiver. We call all the time-wise contributions by the attacker to a particular frame at time t the *attack sequence* and define it as

$$S = (s_1, ..., s_t),$$

where the contribution at time k is

$$s_k = A[k] \cdot P_A[k] \cdot \tilde{P}^{(b_1,...,b_{N_B})}[k].$$

As the attacker proceeds through the attack (i.e, the frame), after each pulse transmission and subsequent disclosure of the actual pulse polarity, he is able to update his knowledge by appending the most recent correlation contribution

$$s_t = \begin{cases} A[t], & \text{if } P_A[t] = \tilde{P}^{(b_1,...,b_{N_B})}[t] \\ -A[t], & \text{if } P_A[t] \neq \tilde{P}^{(b_1,...,b_{N_B})}[t] \end{cases}$$

to the existing attack sequence.

Attack State Although the attacker sees each correlation contribution during the course of the attack, there is still uncertainty in finding to which bit the pulses contribute. Therefore, what we call the attack state, the bit-wise intermediate correlation result, is generally not known to the attacker. However, the attacker can model the attack state as a random variable with a distribution based on the attack sequence. The uncertainty stems from the random reordering, each of which is equally likely from the attacker's point of view. This way, the attack state $(\sigma^1, ..., \sigma^{N_B})$ can be modeled as joint distribution of all N_B bit-wise correlations, each of which can be sampled as

$$\sigma^k \quad = \quad \langle R(S, \pi), \overbrace{(...\|0, ..., 0\| \underbrace{1, ..., 1}_{k\text{-th bit}} \|0, ..., 0\|...)}^{N_B \text{ bits}} \rangle, \quad \pi \quad \overset{UAR}{\leftarrow} \quad \Pi,$$

given a reordering π drawn uniformly at random and some attack sequence S. Sampling each of the N_B correlation values for many reorderings allows the attacker to approximate the probability distribution of the attack state.

If the attacker is in a state with all bit-wise correlations strictly positive, he has won. Therefore, we call these states *winning states*.

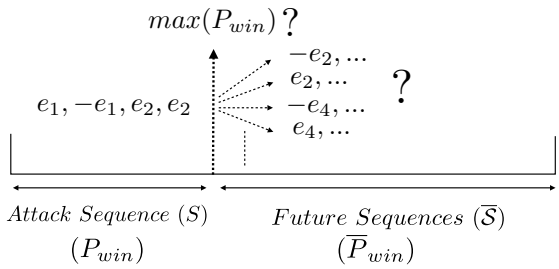


Figure 4.5: The knowledge of a guessing attacker can be split into his assessment of the past and his model of the future.

	$N_p = 4$			$N_p = 8$			$N_p = 16$		
	$N_B = 2$	$N_B = 4$	$N_B = 6$	$N_B = 2$	$N_B = 4$	$N_B = 6$	$N_B = 2$	$N_B = 4$	$N_B = 6$
$\lvert n_{VE}\rvert, \lvert n_{PR}\rvert$ (SPA)	24	20	18	32	24	24	36	28	28
$\lvert n_{VE}\rvert, \lvert n_{PR}\rvert$ (MPA)	68	44	36	140	68	54	294	104	66

Table 4.1: Depending on the attacker and configuration of UWB-PR, different minimum nonce lengths are required to drive the overall attack probability below 10^{-6}. Besides reordering more bits, using longer nonces can serve to compensate the detrimental effects on security by longer symbols (higher N_P).

Current Advantage P_{win} Given some attack sequence and the corresponding state distribution, the attacker is interested in his chances of having already won. This probability we call the attacker's current advantage. Having obtained the probability distribution over all states for an attack sequence S, we can find the current advantage simply by summing the probabilities of all winning states:

$$\sum_{\text{All winning states given S}} P(s)$$

This number essentially represents the attacker's confidence in his past interferences. Because the reordering is unknown, the attacker cannot tell whether he has already won with certainty.

Future Opportunity $\overline{P}_{win}$ At each time during the attack, the attacker can try to look ahead and consider all future progressions of the attack sequence. This involves building a model that serves to estimate his chances

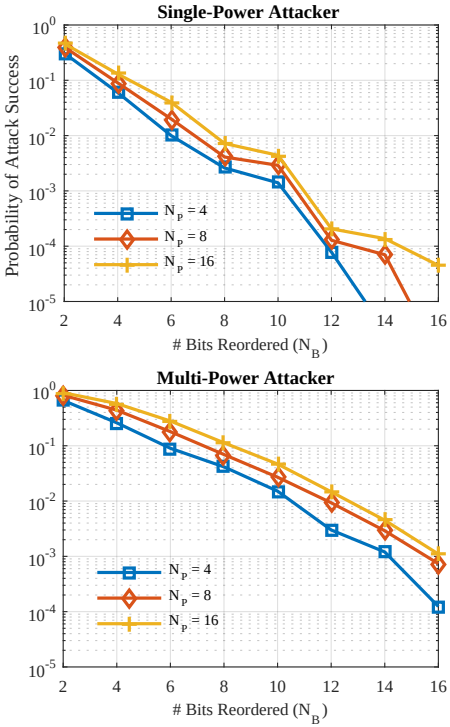


Figure 4.6: Grouping more bits together for reordering (i.e., increasing N_B) makes it harder for both attackers to guess any of the bits, reducing their probabilities of success. This allows compensating for the detrimental effects of longer symbols (higher N_P) on security.

of winning if he continues playing. Evaluating this future opportunity helps the attacker in two ways. First, it allows the attacker to choose his next transmission power optimally, particularly the argument maximizing the future opportunity conditioned on this choice. Second, by comparing the future opportunity against the current advantage, an attacker can make an informed stopping decision during the attack. This means that, if the expected likelihood in the next step are, irrespective of the current energy level choice, worse than the current advantage, the attacker will stop interfering. In any case, building a model for estimating the future opportunity is very complex as it contains uncertainty about the current

state, the reordering, and future pulse polarities. Therefore, it requires the attacker to essentially simulate his own behavior for the entire remaining pulse sequence. Due to the random reordering and pulse blinding, the only information the attacker has about the future is the number of pulses remaining as well as some partial knowledge about the current attack state.

4.3.2 Attack Strategies

The knowledge that informs the strategy of a guessing attacker can be split into past observations and a model for the future, as illustrated in Figure 4.5. However, as discussed previously, guessing attacker's knowledge about future pulses is very limited. We, therefore, argue that any strategy an attacker employs to maximize his success chances is predominantly based on his assessment of the past, *i.e.,* the probability of having won P_{win}. This value will evolve during the attack based on the attacker's guessing luck and the power levels he chooses for his pulses. In terms of strategy, we argue that an attacker's 'degrees of freedom' is given by (i) his decision when to terminate the attack and (ii) the power levels chosen for the pulses. In our model, for the former, we choose an over-approximation on the attacker's knowledge informing the attack termination. The latter we model using two extreme strategies - a *Single-Power* attacker that keeps his transmission level constant throughout the attack and a *Multi-Power* attacker that is not limited in the number of power levels to choose from.

Optimal Attack Termination As the knowledge about the future is very limited, an attacker cannot anticipate if a certain probability of winning can be achieved at any time in the future. Therefore, as an over-approximation for the attacker's capabilities of assessing the future, we assume the attacker to stop at the ideal time w.r.t. his estimate of P_{win}, subject to his energy allocation strategy and a given attack sequence.

Single-Power Attacker (SPA) This is an attacker that sends all pulses at the same transmission power.

Multi-Power Attacker (MPA) This model captures a more powerful attacker that can transmit at varying power levels. Having a limited number of chances to guess a bit correctly, this attacker aims to compensate for any wrong interference as soon as possible. Thus, any pulse guessed wrong will cause this attacker to double his power level for the next transmission. This way, each correctly guessed pulse results in a correct bit. Consequently, each correct guess improves P_{win} and, if things don't go so well, chances of

still guessing the bit remain nonzero as long one pulse for each bit remains (*i.e.,* as long as possible).

Attack Simulation and Results

Both attackers were simulated in MATLAB. For a given (legitimate) polarity sequence, both models result in a deterministic attack sequence. This allowed obtaining attack success probabilities by simulating attacks on randomly sampled polarity sequences and reorderings efficiently. For a sampled polarity sequence, P_{win} was calculated by randomly sampling pulse reorderings. As explained previously, the peak P_{win} over the entire attack sequence was chosen to characterize the attacker's chances of winning for this given sequence (*Optimal Attack Termination*).

Figure 4.6 shows the attack success probabilities for different configurations of N_B and N_P. The results show that security offered by UWB-PR increases for higher numbers of bits grouped for reordering. For the configuration geared towards the long-distance, using 16 pulses per symbol, reordering of all bits reduces the single- and multi-power attacker success to no more than $4.5 \cdot 10^{-5}$ and $1.1 \cdot 10^{-3}$, respectively. The typical length of nonces n_{VE} and n_{PR} as used in distance-bounding protocols amounts to 20 bits. Extrapolating from our results, reordering all 20 nonce bits will decrease the attacker's chances of success further, likely below the 10^{-6} mark for the single-power attacker.

A system implementing UWB-PR faces the choice of how to split up the nonces into groups of bits that are reordered. Either all bits of the nonce can be reordered (i.e. $N_B = |n_{VE}| = |n_{PR}|$), or the nonces can be split into groups before reordering (i.e. $N_B < |n_{VE}| = |n_{PR}|$). Although increasing N_B shows to be the better choice for security, smaller groups might be favorable in some scenarios(such as when memory is limited). Important to note is that this does not necessarily get in the way of overall security, as the nonces can be chosen longer for compensation. In Table 4.1 we list the minimum required nonce lengths for both attackers and different configurations of UWB-PR, such that an attacker's success chances are below 10^{-6}.

4.3.3 Structured Reordering

Giving an attacker partial knowledge about the set of reorderings decreases his chances of winning overall. This becomes evident by comparing previous results (Figure 4.6) to Figure 4.8, which represents simulation results for a partially structured reordering. To understand the impact of the reordering on attack success, we analyze a particular instance of UWB-PR. The idea

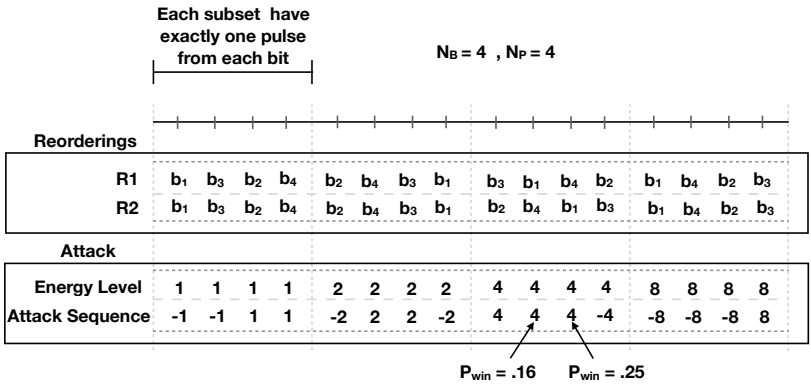


Figure 4.7: Example for Structured Reordering: There are N_P subsets, and each subset has N_B pulses. Each pulse of a subset belongs to a different bit, as is shown by reorderings R1 and R2. In order to maximize the likelihood of correcting any previous negative contributions, the attacker uses the same energy level within the subset and doubles its transmission power upon transitioning from one subset to the next. For the reordering R2, the attack is successful if attack termination happens at the third position of the third subset (at $P_{win} = 0.25$). However, the attack fails for reordering R1, irrespective of the point of termination of the attack.

is to determine the probability of attack success for different numbers of bits reordered under the multi-power attacker model and an optimal attack termination point.

Reordering Process: Instead of reordering all pulses randomly, we follow a specific process. We create N_P subsets, and each subset has N_B pulses, where N_P is the number of pulses per symbol and N_B the number of bits reordered. The N_B pulses of each subset belong to exactly N_B different bits. However, each subset hides the mapping differently by using different reordering and XOR sequences. Figure 4.7 shows an example of this reordering process.

Attack Strategy: The attacker is aware of the statistical distribution, i.e., N_B and N_P, and knows that the N_B pulse of a subset belongs to different N_B bit. This knowledge gives a bias to the attacker; even towards the end of the attack, attacker has non-zero probability of producing a positive contribution on each bit. However, he doesn't know reordering and XOR

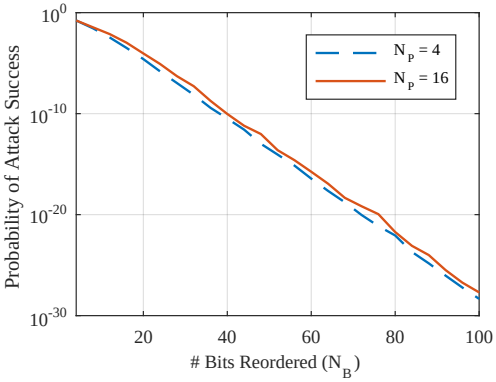


Figure 4.8: Simulation results for structured reorderings: The attack success rates decrease exponentially as the number of bits reordered is increased. The attacker has knowledge about the statistical distribution of bits and pulses, and is given the optimal point of attack termination.

sequence applied on the subset. To maximize the likelihood of positive net power per bit, an attacker needs to decide energy levels for the attack on each pulse and the point of attack termination. For the choice of the energy level, we suggest the following:

- Within a subset, the same energy level is used for each pulse. Given that all pulses belong to different bits, and the attacker does not know the pulse-to-bit mapping, all pulses are equally probable to belong to a certain bit.
- When transitioning from one subset to another, the attacker can decide to use the same, increase or decrease the energy level. Our model chooses the minimum energy level that will maximize the likelihood of positive net power per bit, given that the next pulse polarity is guessed correctly. As long as negative per-bit correlations remain, this is equivalent to doubling the power per pulse upon transitioning.

The energy choice according to this model ensures that the correct guess of a pulse brings the attacker closer to winning, and an incorrect guess can be corrected in the next subset. However, in the process of fixing a wrong interference of a bit, the attacker can end up interfering with another bit. For example, suppose the attacker guesses the polarity of

$(N_B - 1)$ pulses correctly in a subset but guesses one wrong. To maximize his chances of success in the next subset, he needs to guess the polarity of the pulse of this particular bit correctly. In the process of correcting this bit, if the attacker attacks a pulse in the next subset, the probability of correcting this bit is $(0.5 \cdot 1/N_B)$, and causing a negative contribution to another bit is $(0.5 \cdot (N_B - 1)/N_B)$. By increasing the number of bits reordered, the probability of interfering with the wrong bit increases. An attacker also needs to be careful about when to terminate the attack. In the example shown in Figure 4.7, an attacker can stop interfering after the second or third position of the third subset. After interfering with the second pulse of the third subset, the attacker already knows that P_{win} is .16. He can choose to proceed or terminate the attack at this point. For calculating the results, as shown in Figure 4.8, we assume that the attacker continues and terminates the attack at the third position of the third subset, where P_{win} is .25. Results in Figure 4.8 show that the trend of the attack chances for more bits reordered is an exponential decrease. As this captures a scenario in which an attacker has structural knowledge about the reorderings, respectively, the set of possible reorderings is vastly reduced, we conclude that the attacker's success chances must decrease at least exponentially for increased numbers of bits in the general case, too. In other words, the attacker's success probability is negligible in N_B.

4.3.4 Reordering is the Key

Our simulation results show that the number of bits grouped together is an important security parameter, reducing the attacker's success chances rapidly. We can also observe that, for small numbers of bits reordered, the multi-power attacker becomes very strong, guessing the bits with probability close to one if the reordering is done on only two bits. It seems as if security is lost altogether without reordering, despite the attacker not knowing the polarity of individual pulses due to the pulse blinding. Indeed, if a system chooses not to reorder at all, an attacker that can increase transmit power at will has very high chances of guessing the bit. Specifically, he has N_P independent attempts, each with probability 0.5, since he can stop guessing once he has guessed one pulse correctly. The probability of guessing the entire bit follows as $1 - 0.5^{N_P}$, which amounts to 0.99998 for $N_P = 16$. Given that the simulated multi-pulse attacker is essentially an extension of this attacker type over reordered bits, and can be contained for more bits reordered, we argue that the reordering is vital in addressing this existing shortcoming in multi-pulse UWB systems. In consequence, security against

ED/LC attacks requires the reordering to be a shared secret between verifier and prover, and unknown to the attacker.

4.4 Discussion

In this section, we first relate our proposal to the 802.15.4a standard.

4.4.1 802.15.4a with PR?

Until now, we assumed some form of OOK modulation to underly our system. As explained earlier, OOK seems a good fit for our system due to its simplicity. In the following, we investigate if some other modulation, e.g., as used in 802.15.4a, would also suit our requirements and could potentially form the basis of our scheme. To this end, we first describe the assumptions our security features in UWB-PR place on the underlying modulation. At the core of our system, for all security properties, we rely on the modulation consisting of basic energy units that are individually not vulnerable to ED/LC attacks. Typically, such a unit can be thought of as a pulse or group of pulses. These basic energy units have to satisfy the following requirements:

- *Atomicity*: An attacker cannot both detect and interfere with the signal due to its short duration. An ED/LC attack on this unit is therefore not possible.[7]
- *Associativity* w.r.t correlation: All reorderings of a sequence of units result in the same correlation output at the receiver. This is a requirement for guaranteeing the robustness of the system under all possible reorderings.
- *Bandwidth*: Precise ranging asks for high signal bandwidth.

802.15.4a and 802.15.4f both specify UWB PHY modulations with bandwidths upwards of 500MHz. In general, this translates to nanosecond time resolution, which satisfies requirements for centimeter-precision ranging. Therefore, the bandwidth requirement we consider met by both standards. Before we check if the other criteria could potentially be satisfied by 802.15.4a, we introduce some existing issues with its modulation.

[7]Under the assumption that the attacker's processing time is lower bounded by a few nanoseconds.

Security problems of 802.15.4a In its 2007 amendment for ranging, 802.15.4a relies on a mix of BPM and BPSK to accommodate for both coherent and noncoherent transmitters and receivers. In BPM, time-wise coding gain is achieved by repeating a pulse within a short interval many times. In the case of coherent operation, the burst is also associated with a polarity (phase). Fundamentally, and in comparison to 802.15.4f, we can think of basic energy units given by bursts of pulses instead of individual pulses. Due to the high rate of these pulses (499.2MHz) as well as channel multipath, it is unlikely for a non-rake receiver to resolve individual pulses. A receiver will most likely integrate energy over the entire time slot of a burst and obtain timing and phase as an aggregate over all the pulses. This means that the shape of a burst does not contain any relevant information. Individual bursts can, in consequence, become a target for ED/LC attacks due to their unspecific and hence, predictable structure. It has indeed been observed in 802.15.4a [60] that an attacker can always decrease the distance by some value slightly smaller than the distance corresponding to the burst duration.

The standard advocates the use of more pulses per symbol for increased robustness and distance. However, an attacker's distance decrease improves with the amount of such temporal coding gain. This dependency is shown in Figure 4.9 for all mandatory configurations, where it is contrasted with the constantly small decrease possible in UWB-PR [8]. There we also see that at high PRFs, more robustness comes at a high price in terms of security. This effect characterizes the regime of PRF>1MHz, where the power per pulse is limited by the regulatory constraint on average power [108]. Specifically, the comparably high PRFs supported by 802.15.4a are associated with small marginal SNR increases per pulse added. But each pulse added to the burst will proportionally increase its length T_{burst} and give the attacker more time. This results in an unfavorable trade-off between performance and security, especially at high PRFs. Consequently, an 802.15.4a ranging system can be geared towards either security or performance, but not both.

In particular, all configurations place less energy on each pulse than the extended mode of 802.15.4f. This requires configurations to compensate excessively with temporal diversity in order to achieve comparable receive SNR. Indeed, the standard allows for long burst durations of up to roughly 256ns (125 times the minimum), along with proportionally increasing symbol durations. Unfortunately, for the highest mandatory PRF of

[8] In this analysis, we use a simplified model on signal energy under regulatory constraints which do not consider non-idealities of the measurement hardware as introduced in [108].

15.6MHz, this leads to a potential 153.6m and 2461.6m distance decrease by an ED/LC attacker in a coherent or noncoherent setting, respectively. Although one could argue that the option for a shorter burst duration exists, a system opting for robust communication over the long-distance (more than a few meters) will have no other choice than introducing temporal diversity (longer symbol length). This becomes evident in Figure 4.9 when considering the NLoS path loss model, which assumes a $\approx 20\ dB$ signal attenuation to an object (e.g., human body) blocking the direct path. We note that temporal diversity for meaningful operating distances is essential in any UWB system. Since 802.15.4a operates below the peak power constraint of 0dBm per 50MHz, thereby relying on the temporal spreading of transmitting power more than 802.15.4f. The core weakness of 802.15.4a, however, is that temporal diversity can only be gained by increasing the burst duration T_{burst}, which is not secure.

We exemplify this problem by comparing configurations of 802.15.4a and UWB-PR operating over identical bandwidths and allocating similar symbol energy under regulatory constraints. This way, we aim to compare configurations expected to offer similar ranges. With our proposed 16 pulses per symbol and mean pulse repetition frequency (PRF) of 2MHz in UWB-PR, we find in the 802.15.4a-configuration using 32 pulses per burst over a symbol duration of 8205.13 *ns* our closest fit. In the coherent scenario, denoted as 802.15.4a (C), an attacker can decrease the distance by close to 20m, as compared to only less than 1m in UWB-PR. Even worse, if the system chooses not to convey any information in the signal phase, the modulation reduces to pure BPM, and the attacker can guess the symbol value by half a symbol duration in advance [60]. An attacker can then simply adapt his transmission power in the second symbol half to what he observes in the first half of the legitimate symbol. Correspondingly, the maximum distance decrease goes up to 2461.6m in this noncoherent scenario 802.15.4a (NC). This kind of attack represents a fundamental limitation of any noncoherent PPM/BPM system, and its success is independent of the shape and duration of the pulse burst. Both results are listed in Table 4.2, where they are compared to the distance decrease possible under UWB-PR. Irrespective of the configuration chosen in 802.15.4a, higher symbol energy comes at the cost of longer symbol duration which is, in turn, associated with higher distance decreases in a noncoherent setting. This behavior is compared to UWB-PR in Figure 4.9.

We can summarise our insights as follows. With cryptographic reordering and blinding missing, the deterministic time-coding of 802.15.4a and 802.15.4f make both approaches vulnerable to ED/LC

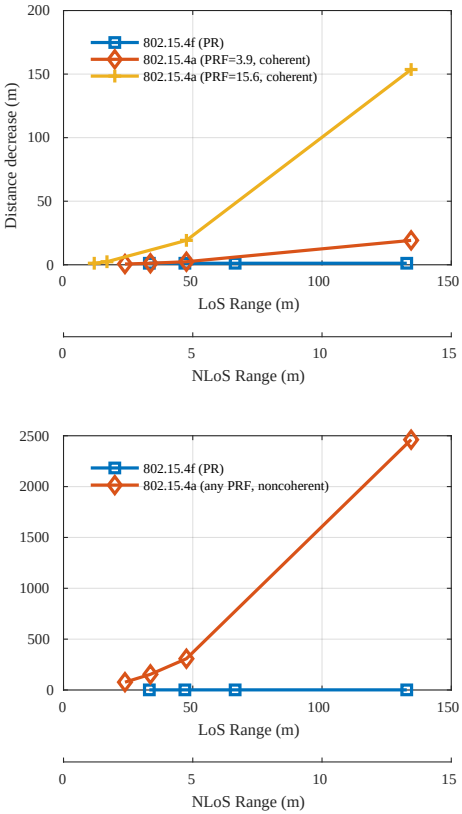


Figure 4.9: Distance decrease in the coherent and noncoherent scenario as a function of the estimated range offered. For comparability, all systems are assumed to use 500MHz bandwidth. NLoS refers to a scenario with 20dB attenuation of the direct path. Non-idealities of the measurement hardware were not considered.

attacks. In 802.15.4f, we find a modulation scheme that provides atomic building blocks that can be effectively interleaved for security. That is why UWB-PR builds on 802.15.4f and introduces reordering of pulses among bit-wise time intervals in order to gain resistance against all physical-layer

	Law	Decrease
802.15.4a (NC)	$\sim 2 \cdot (T_{sym}/2)$	2461.6m (8205.2ns)
802.15.4a (C)	$\sim 2 \cdot T_{burst}$	38.46m (128.2ns)
802.15.4f (PR)	$\sim 2 \cdot T_{pulse}$	1.2m (4ns)

Table 4.2: Ideal, non-guessing distance decrease for coherent (C) and noncoherent (NC) operation of 802.15.4a and our proposed UWB-PR. We assume 16 pulses (802.15.4a) per symbol.

	ISI (IPI)	Precision	Range	ED/LC
802.15.4a	×	√	√	×
802.15.4f (BM)	√	√	×	√
802.15.4f (EM)	√	√	√	×
UWB-PR	√	√	√	√

Table 4.3: UWB-PR is resistant to all physical-layer attacks while avoiding interference among pulses (respectively inter-symbol-interference, when reordering is considered) and providing long communication range.

attacks, including ED/LC attacks. An overview of these considerations is provided in Table 4.3.

4.5 Re-visiting principles for Secure Ranging

With the possibility of distance commitment and cryptographic operations at the physical layer, we need to revisit these principles we discussed in Section 2.4. We will see that the changes in these principles will help in constructing performant and secure ranging systems.

Principle 1. Use a communication medium with propagation speed close to physical limit through space-time, i.e., the speed of light in vacuum. This principle is still valid and is important. Relaxing this constraint will allow the possibility of relay attacks on ToF-based ranging systems.

Principle 2. "Short symbols (preferably one pulse per symbol) are necessary for secure ranging." The restriction of narrow symbols was applied due to the threat of ED/LC attacks, and it has resulted in constraining the communication range of the systems. UWB-PR design showed that longer symbols by performing cryptographic operations at the sample level prevent ED/LC attacks. Therefore, allowing scaling to better performance and increased distance without compromising security. As we

see in the next Chapter, this learning further opened the venue for building techniques that enable distance enlargement attacks detection. However, we have also learned that sample duration should be short (wider bandwidth), and multipath components should not affect signal arriving through the direct path.

Principle 3. "Rapid pulse exchange is necessary for secure ranging." UWB-PR showed that we can send multiple samples constituting multiple bits in a single frame and still achieve secure ranging. By using distance commitment, the receiver performs timing acquisition and then checks for the consistency of the bits with respect to the committed time. To manipulate ToA estimation, an attacker needs to advance/delay the arrival time of all samples by the same time. Due to this check, both single and multi-bit systems have to adhere to the time consistency. We should address performance and resistance to physical layer attacks at the sample level using proper checks at the receiver. This shows that multi-bit challenge-response distance-bounding protocol such as Hu/Perrig/Johnson [109], Sastry/Shankar [110] and Capkun/Hubaux [111] which were considered broken due to ED/LC attacks, are secure if run over a secure physical layer.

Principle 4. "Special bit-error tolerant protocols are required at the logical layer." We showed that while some classes of MTAC like UWB LRP require error tolerance at the logical layer, UWB-PR achieves robustness by increasing symbol duration. UWB-PR is a multi-pulse-multi-bit system that prevents bit errors by increasing the symbol length, i.e., relying on more power per symbol. Error tolerance at the protocol level is therefore not a mandatory requirement for secure distance measurement.

4.6 Conclusion

In this chapter, we presented UWB-PR, a modulation scheme that secures ranging against all physical-layer distance reduction attacks against an external attacker. We provided quantifiable probabilistic security guarantees without making any assumptions regarding channel conditions or the attacker's position. The underlying modulation scheme, pulse repetition frequency, and approach receiver uses to perform ToA estimation and data detection collectively determine if an approach can provide secure ranging. UWB-PR enables a secure modulation scheme for 802.15.4f (or 802.15.4z LRP) that provides data transfer, long-distance ranging without compromising on security. It is, therefore, compatible with the majority of existing distance bounding protocols [19, 23].

Measurements obtained with a prototype implementation of UWB-PR are aligned with that finding.

Chapter 5
UWB-ED: Distance Enlargement Attack Detection in UWB

The advancement of autonomous systems, robots, and cyber-physical systems, and the need to navigate and track them without human involvement, has increased the demand for accurate and secure relative distance measurement - the perceived distance should neither be shortened nor enlarged. Numerous efforts have been directed towards enabling security against distance reduction attacks by redesigning logical and physical layers, *e.g.,* distance bounding, modes of 802.15.4z and UWB-PR *etc.* However, protection against enlargement attacks still relies on dense and often fixed verification infrastructures [112], *e.g.,* towers. Setting them up is expensive and sometimes infeasible; detection of enlargement attack requires the prover to be inside a polygon determined by the verification infrastructure, assuming that none of the measured distances are shortened.

In this chapter, we present *Ultrawideband Enlargement Detection* (UWB-ED)—the first known modulation technique to detect distance enlargement attacks against UWB ranging based on ToF. UWB-ED relies on the interleaving of pulses of different phases and empty pulse slots (*i.e.,* on-off keying). Unable to perfectly guess the phase leaves the adversary with a 50% chance of annihilating pulses (similarly for amplification). As a result, some of the affected (authentic) pulses will be amplified, while others will be annihilated. Unaffected pulses will remain intact, while positions that originally had no pulses may now have adversary-injected ones. The technique presented herein gets the receiver to seek evidence indicating whether such a deformed trail of pulses in the transmission was indeed authentic, albeit corrupt.

Similar to the UWB-PR in the previous chapter (which addresses distance-reduction attacks), we leverage a randomized permutation of pulses. However, unlike UWB-PR, we cannot simply look for whether these are out of order and ignore them because that is precisely the adversary's objective in distance-enlargement - misleading the receiver to ignore the authentic signals. Instead, UWB-ED checks the *energy distribution* of pulses, comparing the aggregate energies of a subset of pulses at the positions where high energy was expected (as per the sender-receiver secret pulse-permutation agreement) with others where low energy was

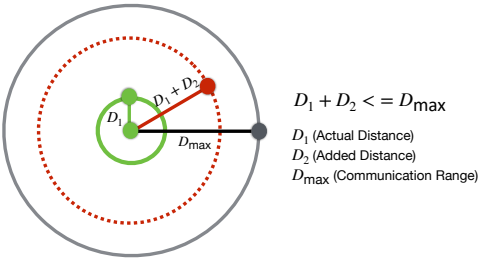


Figure 5.1: If $D_1 + D_1 > D_{\max}$, the devices realize they are outside each other's communication range without the need to run distance-enlargement detection protocol.

expected. To subvert this detection approach, the attacker would be forced to inject excessive energy throughout the whole transmission, which could then be detected using standard DoS/jamming-detection techniques.

We derive the probability of an adversary succeeding in a distance-enlargement attack against UWB-ED. This is also useful in setting input parameters, *e.g.,* balancing an application's security requirements and ranging rate while accounting for channel conditions. For example, we show how proper parameterization of UWB-ED limits an adversary's success probability in enlarging distances to $< 0.16 \times 10^{-3}$.

In summary, this chapter's contributions are twofold.

- UWB-ED—a novel, readily-deployable modulation technique for detecting distance enlargement attacks against UWB ToF ranging systems, requiring absolutely no verification infrastructure, and making no impractical assumptions limiting adversarial capabilities.
- Analytical evaluation to UWB-ED, where the probability of adversarial success is derived as a function of input parameters and channel conditions. This evaluation is also validated using simulations.

5.1 UWB-ED Design

UWB-ED consists of two phases conducted between both devices: Distance Commitment and Distance Verification. Figure 5.2 shows a timing diagram of both phases. In the first, the devices measure the distance between them using a two-way ranging protocol. The distance measured in this phase should not exceed the supported communication range D_{max}, *i.e.,* $t^c_{tof} < t^{max}_{tof}$. If measured distance $D_1 + D_2$ is longer than the D_{max}, the

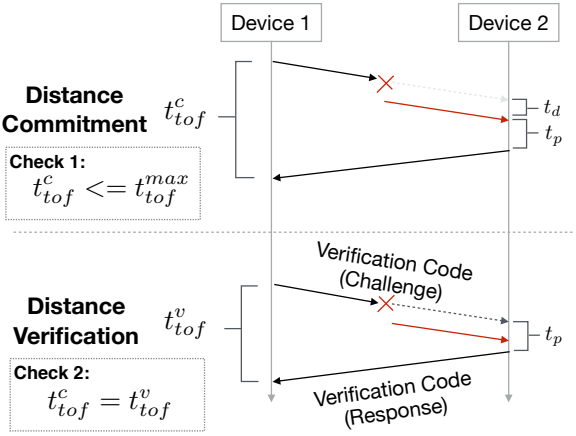


Figure 5.2: Timing diagram of UWB-ED operation. See inline (Section 5.1) for notation.

device realize that they are not within the communication range and they are communicating through a relay, therefore, the measured distance is discarded. In the distance verification phase, the devices measure their distance by exchanging verification codes (generated using a special UWB-ED modulation). To detect enlargement attacks, devices look for distorted traces of that code. The attack is detected when such traces are found, $t^c_{tof} > t^{max}_{tof}$, or when $t^c_{tof} \neq t^v_{tof}$ (Fig. 5.2). By enlarging distance in the commitment phase, the adversary increases t^c_{tof} by t_d, but fails to enlarge the distance in the verification phase. Annihilation attempts on the challenge frame are shown, but the adversary can also attack responses from both devices.

Distance Commitment Phase. The devices measure secure upper bound by using distance bounding along with secure modulation techniques such as UWB-PR. This provides strong guarantees against reduction attacks but is susceptible to enlargement attacks. The distance committed in this phase should not exceed the communication range (*i.e.,* an enlargement attack is detected when $t^c_{tof} > t^{max}_{tof}$). This check ensures that the nodes can communicate without a relay. An adversary enlarging distance by more than the communication range is also exposed using this check.

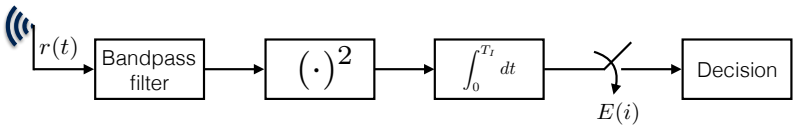


Figure 5.3: Non-coherent energy detector receiver.

Distance Verification Phase. In this phase, the committed distance is verified, *i.e.,* an enlargement attack is detected when $t^c_{tof} \neq t^v_{tof}$. To achieve this, the devices measure their distance using round-trip time-of-flight, with both challenge and response messages protected using specially crafted *verification codes* (*i.e.,* special UWB-ED modulation). In this exchange, the sender initiates the distance verification phase by transmitting a verification code; the receiver tries to detect the presence of that code, or traces thereof, in the transmission, despite the adversary's efforts to *trail-hide* its existence from the channel (Section 3.3). The code and check is applied to both time-of-flight messages. Both devices first agree on the code's structure as follows.

5.1.1 Modulation/ Code Generation

Code length. The code consists of n positions, α of which have energy, and the remaining $\beta = n - \alpha$ are empty, *i.e.,* absent of pulses (conceptually similar to OOK modulation, where $\alpha = \beta$). The code length affects the performance and security of the presented modulation technique. Larger α and β values improve the security by reducing the probability of adversarial success in mounting undetectable distance-enlargement attack. However, increasing the code length reduces the frequency of conducting two-way ranging. Additionally, the Federal Communications Commission (FCC) imposes restrictions on the number of pulses with energy, effectively limiting α per unit of time. As such, β could be independently increased to compensate for the loss of code length. Setting these parameters is discussed in Section 5.2.

Pulse phase. The sender uses a random phase for the α pulses it transmits. Each phase is equally likely. The phase will be irrelevant for the receiver because energy detector (ED) receivers shown in the Figure 5.3 are agnostic to the phase [113]. Such receivers are commonly used by the 802.15.4f and LRP mode for the UWB ranging. The energy detector receiver

is consists of a square-law device to compute instantaneous received signal power and an energy integrator. For the received signal $r(t)$, the output of the receiver can be expressed as:

$$E(k) = \int_{T}^{T+T_I} [r(t)]^2 dt \tag{5.1}$$

where T is the integration start time, T_I the integration window size. These receivers perform squaring and integration, making phase information irrelevant for pulse detection. The sender therefore need not share the phase of the pulses with the receiver.

Pulse permutation. The sender and receiver secretly agree on a random permutation of the n positions, obtained from a uniform distribution. Figure 5.4 shows an example before and after the permutation. The verification code can thus be considered a sequence of $\{-1, 0, 1\}$ pulses, where $\{-1, 1\}$ represent the phase, and $\{0\}$ pulse absence.

Spacing between pulses. We submit that spacing between pulses T_s should be such that $T_s > 2d/\mathbf{c}$, where d is the distance between two devices. if an adversary replays signal after the spacing (*i.e.,* $T_D \geq T_s$), the attack is detected due to the maximum distance constraint (D_{max}) imposed in the distance commitment phase. The adversary would thus replay its delayed version of a pulse within the T_s time window to avoid being detected. As such, legitimate pulse i will not overlap with the adversary's delayed version of pulse $i-1$, or any further adversary pulses $i-2$, $i-3$, *etc.* Therefore, an attacker can try to annihilate the legitimate signal and replay it after a delay T_D, where $T_D < T_s$.

An example code structure, and adversarial attempts to corrupt and replay it, is shown in Fig. 5.5.

5.1.2 Verification

Upon receiving a transmission, the receiver starts processing the code associated with the highest preamble's peak. The code associated with a peak is the train of T_s-spaced pulses that start at a fixed time interval (*e.g.,* agreed upon between the sender and receiver) after the peak. This peak however may not be authentic, and could be the adversary's replayed version. The receiver thus backtracks at fixed time steps corresponding to

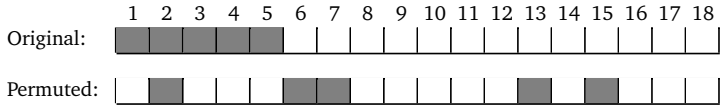


Figure 5.4: An example verification code with a randomly-looking pulse reordering, where $\alpha = 5$, $\beta = 13$, and the code contains $n = \alpha + \beta = 18$ pulses. Upon receiving the permuted code pulses as per the secret agreement between the sender and receiver, the receiver knows that Bin_α will contain the received energies at the positions (gray) {2, 6, 7, 13, 15}, which are the expected high-energy pulses. Bin_β will contain the rest: {1, 3, 4, 5, 8, 9, 10, 11, 12, 14, 16, 17, 18}.

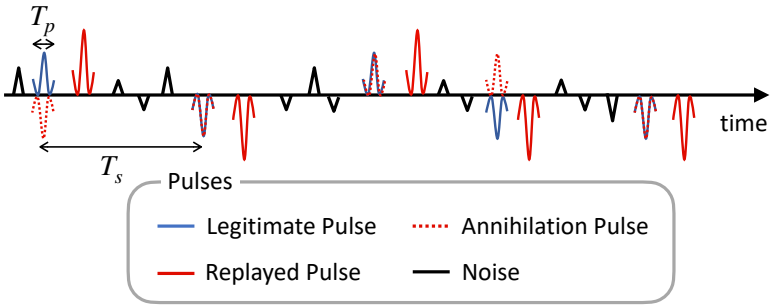


Figure 5.5: An example verification code of n slots (9 of which are shown), the spacing T_s between consecutive pulses is $1\mu s$ and pulse width T_p is $2ns$. An adversary transmits a pulse to distort the legitimate pulse (dashed red). The adversary also replays the authentic signal with the delay T_D (solid red). Best viewed in color.

the pulse width T_p (*e.g.,* 2 *ns*), trying to identify if another version of the code (or a possible distorted imprint of it) was present in the transmission at an earlier time. The receiver does not need to backtrack further beyond some time T_0, knowing the maximum communication range. If the last distance verification occurred recently, the verified range could be used (in combination with the devices' upper bound motion speeds) to reduce the backtracking time.

Backtracking requires the receiver to record transmissions. If an earlier version of the code is found (and their difference exceeds the receiver's standard precision, *e.g.,* ± 10 *cm* for DecaWave [38]), it is used for ToF estimation.

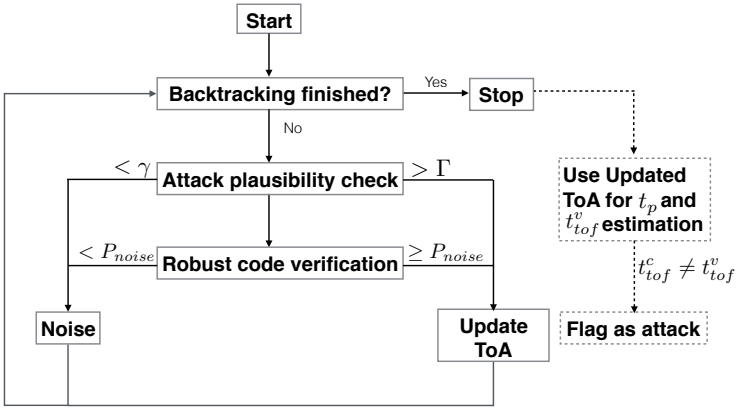


Figure 5.6: The receiver backtracks to detect enlargement attacks. An event is flagged as an attack when the aggregate energy is higher than Γ (*e.g.,* DoS, jamming), *i.e.,* the data looks more similar to a verification code than noise. The last flagged position is used for the ToF estimation.

As shown in Fig. 5.6, the receiver performs Attack Plausibility check and Robust Code Verification to detect attacks until the maximum backtracking time is reached. For each code, the receiver does not look for an exact match of the transmitted pulses in their positions simply because that could be easily bypassed with minimal adversarial efforts. Instead, the receiver proceeds as follows. Knowing the mapping of the pulse positions, the receiver distributes the received powers of each pulse among two bins, Bin_α and Bin_β. The former will have the values of the received power (*e.g.,* in Watts) of the energy-present pulse positions, the latter energy-absent positions (Fig. 5.4).

Attack Plausibility check. For each candidate verification code obtained during backtracking, the overall received signal power (the aggregate of Bin_α and Bin_β) is measured, and compared to a predefined threshold, γ. This threshold is based on the receiver's noise figure. If the aggregate exceeds γ, a potential verification code has been found. Otherwise it gets discarded as noise. The aggregate energy is then compared to another threshold, Γ. This is calculated based on the overall aggregate energy the receiver expects to receive based on the measured distance in the commitment phase, following the path loss model. Artificial distance enlargement caused by the adversary in the commitment phase lowers

the receiver's calculated Γ (because of the higher path loss), thus increases the likelihood of the actual received aggregate to exceed Γ. If the aggregate exceeds Γ, an adversary may possibly be injecting energy into the channel to distort the authentic code. If the verification code is neither discarded as noise ($< \gamma$) nor exceeds Γ, the receiver proceeds to the Robust Code Verification check.

Robust Code Verification. Now the receiver checks the verification code content. If the receiver simply flags the presence of one or more pulses (above noise) in Bin_β as an attack, false positives increase because such pulses could occur for many legitimate reasons (*e.g.,* noise spikes, reflections, interfering transmissions, antenna orientation, or multipath).[1] Instead, the receiver performs a sequence of binary hypothesis tests on random pulse samples. It tests if the candidate code is more similar to an authentic code than noise. It chooses $r \leq \alpha$ random pulses from the α in Bin_α (where r is the number of pulses per symbol), aggregates their received powers and compares that to the aggregate of another r pulses randomly chosen from the β in Bin_β. If the aggregate of those selected from Bin_α is larger, the receiver identifies this as a candidate authentic code, and records its ToA. Finally, the distance is calculated based on the recorded ToA of the most recently received code, and a mismatch with the committed distance is flagged as an attack.

A candidate verification code could be again noise, which has slipped the Attack Plausibility check perhaps due to some sporadic noise spikes in the transmission. Noise has a probability of $\leq P_{\text{noise}}$ to satisfy the Robust Code Verification check, where P_{noise} is derived as (5.31) in Section 5.2.1. As such, the receiver estimates the probability that the above condition is satisfied. This is done by repeating the random sampling υ times, and checking if the ratio of the number of times the condition is satisfied to υ exceeds P_{noise}. This would indicate the code is not noise, and is either authentic or adversary-replayed. Regardless, the receiver uses the ToA of the most recent code found.

5.1.3 Setting the Energy Thresholds.

Setting the upper-bound threshold, Γ. To set Γ, the receiver relies on the committed (unverified) distance between itself and the sender. This dictates

[1] If the receiver instead interprets a pulse in Bin_β as an indication that the code is not authentic and continues backtracking, it may very well skip the authentic code thus helping the adversary.

the path loss—the amount of power loss per pulse as pulses propagate the medium. Larger committed distance causes the receiver to expect less power, thus setting a lower Γ. Thus, by increasing the committed distance, the adversary helps divulge its malice.

The path loss function $f()$ for outdoor UWB LoS is [114]:

$$f(d) = PL_0 + 10 \cdot n \cdot log\left(\frac{d}{d_0}\right) \tag{5.2}$$

where d is the distance in meters, and PL_0 is a constant representing the path loss at the reference distance d_0. For UWB LoS channel model, these constants are set to [114]:

$$f(d) = -46.3 - 20\ log(d) - log\left(\frac{6.5}{5}\right) \tag{5.3}$$

This is calculated in the standard signal ratio unit, dB, where:

$$\text{Power ratio (in } dB) = 10\ log\ (\text{ratio}) \tag{5.4}$$

The path loss function thus expresses the power loss as

$$f(d) = 10\ log\left(\frac{(\lambda_b)^2}{(\lambda_{\text{sent}})^2}\right) \tag{5.5}$$

or

$$\frac{(\lambda_b)^2}{(\lambda_{\text{sent}})^2} = 10^{f(x)/10} \tag{5.6}$$

where $(\lambda_b)^2$ is the pulse instantaneous power the receiver *expects*, and $(\lambda_{\text{sent}})^2$ is that the sender has actually sent, *e.g.,* both in Watt. Knowing the constant pulse power of the sender, then the pulse power is expected to be received as:

$$(\lambda_b)^2 = (\lambda_{\text{sent}})^2\ 10^{f(x)/10} \tag{5.7}$$

The receiver then calculates Γ as follows:

$$\Gamma = \alpha\ (\lambda_b + N)^2 + \beta\ (N)^2 \tag{5.8}$$

where d is the (unverified) distance in meters between the sender and receiver obtained at commit stage, either true or artificially enlarged in case of an attack. N is an instantiation of zero-mean Gaussian noise at the receiver, *i.e.,* the noise present in the receiver's channel and cannot be removed [115].

There are other factors that contribute to the degradation of power. These factors could cause further power loss E, typically up to $E = -8\ dB$ more [116, 117]. If the receiver sets Γ as that after the expected further degradation (*i.e.,* too small Γ value), false positives may increase because such additional signal-degradation factors may or may not occur—if they do not, the receiver would then falsely assume such relatively "too high" aggregate energy is due to an attempted attack. Accordingly, the receiver sets Γ based only on the (almost certain) path loss deterioration. Any further power loss would then be added benefit to the adversary, as it allows the adversary to inject more pulses into the channel to corrupt the authentic code without exceeding Γ.

Setting the lower-bound threshold, γ. If the aggregate energy is $< \gamma$, it would be either due to noise or a substantial deterioration of the authentic signal where no meaningful information could be recovered during the Robust Code Verification. Too high γ leads to false negatives; too low triggers Robust Code Verification even for noise. For critical applications seeking to prevent false negatives, γ could be set conservatively based on the receiver's noise variance σ_N^2:

$$\gamma = (\alpha + \beta) \cdot \sigma_N^2 \tag{5.9}$$

5.1.4 Attack Resilience

Here we explain how UWB-ED resists standard enlargement attacks. More complex attacks are discussed in Section 5.3.

Detecting Signal Replay

An adversary that simply replays authentic pulses does not win because the receiver backtracks to detect earlier copies of the code. UWB-ED provides resilience to benign signal distortion, *e.g.,* due to channel conditions or antenna orientation, because the receiver looks for similarities between the code and the received signal (versus exact data match), allowing for a higher bit error rate. In general, poor channel conditions (low SNR) can be compensated for by increasing the symbol length, r, minimizing the bit error rate.

Complicating Signal Annihilation

The unpredictability of the pulse phase means an adversary must either wait to detect it and immediately inject the reciprocal pulse for annihilation,

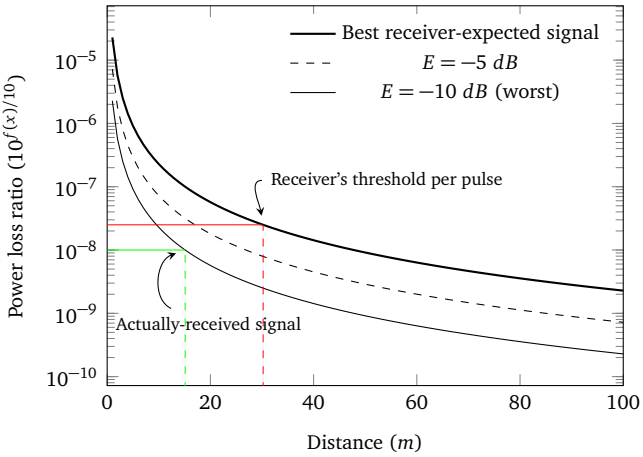


Figure 5.7: The best expected signal power as calculated by the receiver using the path loss function in (5.3), the signal at $E = -5\ db$ of further power loss, and at $E = -10\ db$ (worst expected). If the distance is $D_1 = 15.11\ m$ (green line), and the adversary doubles it, *i.e.,* by adding $D_2 = 15.11\ m$ to make it $D_1 + D_2 = 30.22\ m$ (red line), the receiver will set the threshold following the fake distance, at $10^{f(D_1+D_2)/10} = 10^{-7.6}$. The adversary's room is the difference between the red and green lines on the y-axis. At $D_2 = 32.68\ m$, the adversary has no room. Best viewed in color.

or inject a random-phased pulse hoping it is the reciprocal. The former is infeasible in practice for UWB (see Section 2.2). The latter results in amplifying or annihilating the authentic pulse, each with a 50% chance. Amplification is unfortunate to the adversary, as the adversary now needs to compensate with an equivalent amplitude, A. Amplification doubles the amplitude. The estimated energy of the pulses will thus amount to $\sim A^2$, and the adversary-contributed amplification to $\sim (2A)^2$.

Since the result is indeterministic for the adversary, it leads us to the next discussion: how successful would the adversary be in "contaminating the evidence" that an authentic verification code existed, and how much energy room does the adversary have to do that before exceeding Γ?

Mitigating Evidence Contamination

To hide the authentic code, the adversary tries to inject energy into the channel, hoping it annihilates as many of Bin_α pulses as possible. We thus calculate the room available to the adversary here, and use that to

derive the probability of adversarial success in distance enlargement in Section 5.2.

Figure 5.7 shows the path loss function in (5.6) as used by the receiver to detect the threshold Γ, as well as the worst receiver-expected signal after additional deterioration. The receiver sets the threshold based on the best expected signal. The room available for the adversary to add energy depends on the actual signal received. The most favorable situation to the adversary is when the received signal power is the worst (lowest E), which allows the adversary to inject pulses without exceeding Γ. For example, in Fig. 5.7, if the actual distance between the sender and receiver is $D_1 = 15.11\ m$ (green line), and the adversary is trying to add $D_2 = 32.68\ m$ to make the distance $D_1 + D_2 = 47.79\ m$ (red line), the receiver will set Γ using the fake distance, $D_1 + D_2$. At such a relatively large added distance, D_2, the received pulse power is unlikely to fall below $f(D_1) + E = 10^{-8}(\lambda_{\text{sent}})^2$ at, *e.g.,* $E = -10\ dB$. The room available to the adversary to inject energy becomes too small, significantly reducing its chances of success.

The room-per-pulse, R, available to the adversary to enlarge the distance thus lies in-between the received signal and Γ, and is calculated in dB as:

$$R = f(D_1 + D_2) - (f(D_1) + E) \tag{5.10}$$

where E represents other channel degrading factors, and the distances D_1 and D_2 (in meters) are respectively the true distance between both devices, and the extra distance the adversary intends to add. This room is thus expressed as:

$$\zeta = 10^{R/10} \tag{5.11}$$

Figure 5.8 plots ζ at various distance ratios D_2/D_1.

Recall that the adversary may succeed to annihilate some of the pulses falling in Bin_α. But since Bin_β in the authentic code have nothing but noise, adding pulses into those will result in an increase in the overall aggregate energy. As such, this available energy room in (5.10) by itself does not give a perfect indication to the adversary's chances of success.

5.1.5 A Numerical Example

Figure 5.9 shows an example verification code, expanded from Fig. 5.4, where the adversary injects $k = 10$ random-phased pulses. For simplicity, the figure assumes $N = 0$. If the distance between the sender and receiver is $D_1 = 4\ m$, and the adversary is trying to enlarge it by $D_2 = 4.5\ m$ to make it $D_1 + D_2 = 8.5\ m$, and assuming $(\lambda_{\text{sent}})^2 = 7.6\ \mu W$, then the receiver

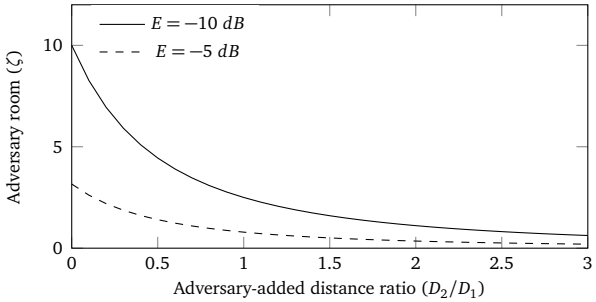


Figure 5.8: Adversary's room to add energy, ζ in (5.11), against the ratio of the adversary-added to true distance (D_2/D_1); E represents additional signal degradation beyond path loss.

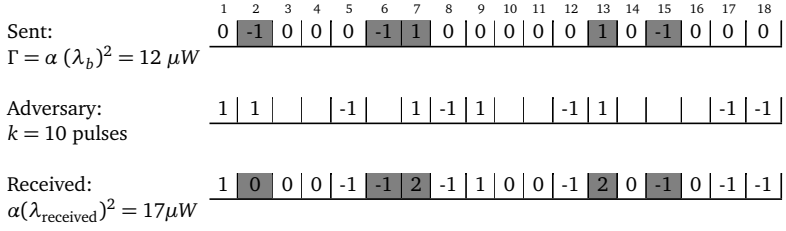


Figure 5.9: An example of the random-phased Bin_α pulses (dark gray) reordered following the permutation in Fig. 5.4. After the adversary injects $k = 10$ random-phased pulses at random positions, the receiver will get the summation at each pulse position.

expects a best case received power of:

$$\begin{aligned}(\lambda_b)^2 &= (\lambda_{\text{sent}})^2\ 10^{f(D_1+D_2)/10} \\ &= 7.67 \times 10^{f(8.5)/10} = 2.4\ \mu W\end{aligned} \tag{5.12}$$

From (5.9) at $N = 0$ and $\alpha = 5$ (as in Fig. 5.9), it then calculates the threshold as:

$$\Gamma = \alpha\ (\lambda_b)^2 = 12\ \mu W \tag{5.13}$$

At $E = -10\ dB$, the actual signals are received as:

$$(\lambda_w)^2 = (\lambda_{\text{sent}})^2\ 10^{(f(D_1)+E)/10} \approx 1\ \mu W \tag{5.14}$$

Now assuming the adversary is $D_3 = 6\ m$ away from the receiver, and uses a random-phased pulse with transmission power of $(\lambda_{\text{sent}}^{\text{adversary}})^2 =$

15.77 μW. At $E = -10\ dB$, the receiver would receive the adversary's signals as:

$$(\lambda')^2 = (\lambda_{\text{sent}}^{\text{adversary}})^2\ 10^{(f(D_3)+E)/10} \approx 1\ \mu W \tag{5.15}$$

So in the best case for the adversary, where the signal is highly deteriorated, the adversary would then have a per-pulse room of $R = 3.45\ dB$ to add energy, which amounts to 7 μW more, *i.e.,* up to $\Gamma = 12\mu W$. In Fig. 5.9, after the adversary injects its $k = 10$ pulses at the example random positions and with the random phases shown, it results in annihilating a single pulse (at position 2), amplifying two pulses (at positions 7 and 13), and adding seven more 1 μW pulses for an increase of the overall aggregate to be 17 μW. This exceeds $\Gamma = 12\ \mu W$, and this attack would thus be detected.

5.2 Security Analysis

We evaluate UWB-ED by deriving the probability of success for an adversary enlarging the distance. We also validate that model using simulations in Section 5.2.2.

5.2.1 Probability of a Successful Attack

The adversary hides the authentic code by having the aggregate of the r pulses that the receiver chooses from Bin_β exceed Bin_α. The adversary must also avoid injecting too much energy to not exceed Γ. Not knowing which pulse belongs to which bin, the adversary injects k pulses at random positions thus affecting k of the n pulses in the code.

To that end, the probability of mounting a successful attack, P_{sa}, is the intersection of the probability of two events (the checks in Fig. 5.6): the aggregate of the energy pulses chosen from Bin_β ($b\beta$) exceeds that of Bin_α ($b\alpha$), and the added energy is $\leq \Gamma$:

$$P_{\text{sa}}(\alpha, \beta, r, \Gamma, k) = P_{b\beta > b\alpha}(\alpha, \beta, r, k) \cap P_{\leq \Gamma}(\alpha, \beta, k) \tag{5.16}$$

Probability of successfully evading the Robust Code Verification check ($P_{b\beta>b\alpha}$)

To evade this, the adversary must have an energy aggregated from Bin_β exceed Bin_α. When the adversary injects k pulses into the channel, x will fall into Bin_α, and the remaining $k-x$ into Bin_β. $P_{b\beta>b\alpha}$ is then the probability of this distribution occurring multiplied by the probability of the attack succeeding under this distribution, for all possible such distributions

$0 \leq x \leq \alpha$ and $0 \leq k-x \leq \beta$. To calculate the probability of the distribution occurring, consider the general case of a bucket containing two types of objects (*e.g.,* colored pearls): I of the first type, and J of the second. If ψ objects are selected at random, the probability that i and j of the ψ are respectively of the first and second type ($i+j=\psi$) is:

$$\frac{\binom{I}{i}\binom{J}{j}}{\binom{I+J}{i+j}} \tag{5.17}$$

where $\binom{n}{r}$ denotes n choose r and is given by:

$$\binom{n}{r} = \begin{cases} \dfrac{n!}{r!(n-r)!}, & 0 \leq r \leq n \\ 0, & \text{otherwise} \end{cases}$$

Similarly, the probability that x and $k-x$ of the adversary's k pulses respectively affect the α in Bin_α and β in Bin_β is:

$$\frac{\binom{\alpha}{x}\binom{\beta}{k-x}}{\binom{\alpha+\beta}{k}}$$

For all possible such distributions, we have:

$$P_{b\beta>b\alpha}(\alpha,\beta,r,k) = \sum_{x=0}^{\alpha}\left(p_{\alpha,\beta,r,k}(x)\cdot\frac{\binom{\alpha}{x}\binom{\beta}{k-x}}{\binom{\alpha+\beta}{k}}\right) \tag{5.18}$$

where $p_{\alpha,\beta,r,k}(x)$ is the probability $b\beta > b\alpha$ given the adversary affected x and $k-x$ pulses in Bin_α and Bin_β respectively.

To derive $p_{\alpha,\beta,r,k}(x)$, we assume for simplicity a unity power-per pulse, *i.e.,* the sender's and the adversary's pulses reach the receiver after path loss and other factors at a constant energy of $\pm 1\mu W$.[2] This is similar to the example given in Fig. 5.9. Every adversary-added pulse in Bin_β will result in a 1 μW of added energy from the receiver's point of view since the receiver's aggregation is agnostic to a pulse's phase. For Bin_α, after the adversary affects x pulses, some will be annihilated while others will be amplified. From the receiver's point of view, after the adversary's pulses are injected, Bin_α will have a mix of $2^2 = 4\mu W$ and 0 μW (adversary-affected) pulses, as well as the original 1 μW unaffected pulses.

[2] Analogous analysis applies for non-constant energy.

More 0 μW (annihilated) pulses in Bin_α raises the chances that $b\beta > b\alpha$, which is in the adversary's favor. Since every affected pulse in Bin_α will either result in a 0 μW or a 4 μW pulse, there are 2^x possible outcomes. Of those, there are $\binom{x}{g}$ ways that g 0 μW pulses will occur. The probability that the x adversary-injected pulses that fell in Bin_α result in a annihilation of g pulses is thus $\binom{x}{g}/(2^x)$. For all possible numbers of annihilated pulses $0 \leq g \leq x$, the adversarial success probability in the event that x fell in Bin_α is:

$$p_{\alpha,\beta,r,k}(x) = \sum_{g=0}^{x} \left(p_{\alpha,\beta,r,k,x}(g) \cdot \frac{\binom{x}{g}}{2^x} \right) \tag{5.19}$$

where $p_{\alpha,\beta,r,k,x}(g)$ is the probability $b\beta > b\alpha$ given g annihilated pulses in Bin_α.

When Bin_α has g annihilated (0 μW), $x-g$ amplified (4 μW), and $\alpha - x$ unaffected pulses (1 μW), the probability of $b\beta > b\alpha$ in the event x fell in Bin_α, and g of the x pulses were annihilated is the probability that an aggregate of $m-1$ is chosen from Bin_α and an aggregate of $\geq m$ is chosen from Bin_β. For each possible $0 \leq y_1, y_2 \leq r$, we have:

$$p_{\alpha,\beta,r,k,x}(g) =$$

$$\sum_{y_1=0}^{r} \sum_{y_2=0}^{r} \left(\frac{\binom{g}{y_1}\binom{x-g}{y_2}\binom{\alpha-x}{r-y_1-y_2}}{\binom{\alpha}{r}} \cdot \sum_{i=m}^{r} \frac{\binom{k-x}{i}\binom{\beta-(k-x)}{r-i}}{\binom{\beta}{r}} \right) \tag{5.20}$$

where m is:

$$\begin{aligned} m &= 0^2 \times y_1 + 2^2 \times y_2 + 1^2 \times (r - (y_1 + y_2)) + 1 \\ &= r - y_1 + 3y_2 + 1 \end{aligned} \tag{5.21}$$

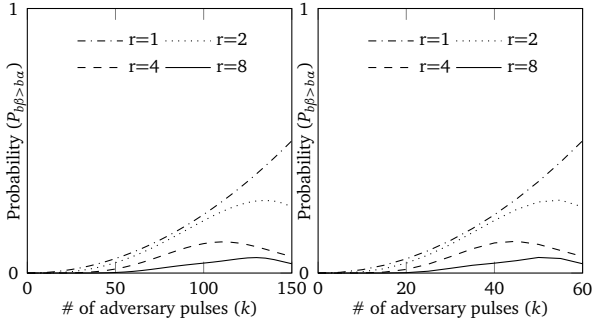
At $r = \alpha$ (*i.e.,* selecting all Bin_α pulses) and $\alpha \leq \beta$, we get:

$$p_{\alpha,\beta,r,k,x}(g) = \sum_{i=m'}^{r} \frac{\binom{k-x}{i}\binom{\beta-(k-x)}{r-i}}{\binom{\beta}{r}} \tag{5.22}$$

where m' is:

$$\begin{aligned} m' &= 2^2 \times (x-g) + 1^2 \times (\alpha - x) + 1 \\ &= 4(x-g) + (\alpha - x) + 1 \end{aligned} \tag{5.23}$$

Figure 5.10 plots $P_{b\beta > b\alpha}$, where $\alpha = 50$. From these results, increasing β is not necessarily effective for the Robust Code Verification check to detect



(a) $\beta = 100$ (b) $\beta = 10$

Figure 5.10: Probability that the Robust Code Verification check fails to detect the adversary's attack, plotted using (5.18) in Section 5.2.1, at $\alpha = 50$ and $0 \leq k \leq \alpha + \beta$.

attacks, since the adversary maintains its success probability by increasing k proportionally; there is a visually similar pattern of adversarial success probability in both Fig. 5.10a and 5.10b. As such, the advantage of the empty pulses in Bin_β does not quite manifest in the Robust Code Verification check, rather the Attack Plausibility check.

Another observation is that higher r lowers the adversary's success probability. For example at $\beta = 100$ (Fig. 5.10a), the adversary has a 27% chance at $r = 2$ (which occurs at $k = 135$), versus 5.85% at $r = 8$ (at $k = 130$). In Section 5.2.1, we show that at $r = \alpha$, we get the optimal security results.

Final Probability of Adversary's Success

In (5.16), the event that the aggregate energy after the adversary's pulses is $\leq \Gamma$ and the event that $b\beta > b\alpha$ are dependent, and thus their intersection is not their product. Recall that in (5.19), g is the number of annihilated pulses, $x - g$ is the number of amplified pulses in Bin_α, and $k - x$ is the number of added pulses in Bin_β. The aggregate-energy does not exceed Γ when the adversary's pulses satisfy the inequality:

$$\begin{aligned}&(k-x)\,(\lambda' + N)^2 + (x-g)\,(\lambda' + \lambda_w + N)^2 + \\ &(\alpha - x)\,(\lambda_w + N)^2 + (\beta - (k-x) + g)\,(N)^2 \leq \Gamma\end{aligned} \tag{5.24}$$

where λ' is defined as in (5.15), and Γ in (5.9).

If the adversary uses a variable pulse power randomly chosen from a distribution with a mean much different from λ_w, authentic pulses colliding with their reciprocal will not be fully annihilated. The adversary thus sets its power such that its mean at the receiver matches the sender, *i.e.,* $\overline{(\lambda')^2} = (\lambda_w)^2$. Assuming $(\lambda_w)^2 = (\lambda')^2$ in (5.24), we get:

$$k + 2x - 4d + \alpha \leq \frac{\alpha\ \lambda_b^2 - \epsilon}{\lambda_{\mathrm{w}}^2} \tag{5.25}$$

where ϵ is a representation of noise, and evaluates to:

$$\epsilon = N\ (\lambda_w\ (2k + 2\alpha - 4g) - \lambda_b(2\alpha))$$

As $\epsilon \to 0$, (5.25) becomes:

$$k + 2x - 4d \leq \alpha \left(\frac{\lambda_b^2}{\lambda_{\mathrm{w}}^2} - 1 \right) \tag{5.26}$$

From (5.12) and (5.14), we have:

$$\begin{aligned} \frac{\lambda_b^2}{\lambda_{\mathrm{w}}^2} &= \frac{(\lambda_{\mathrm{sent}})^2\ 10^{f(D_1+D_2)/10}}{(\lambda_{\mathrm{sent}})^2\ 10^{(f(D_1)+E))/10}} \\ &= 10^{(f(D_1+D_2)-(f(D_1)+E))/10} \\ &= \zeta \end{aligned} \tag{5.27}$$

where ζ, from (5.11), represents the room-per-pulse available to the adversary to add energy into the channel.

We now calculate $p_{\alpha,\beta,r,k}(x,\Gamma)$, similar to (5.19) as:

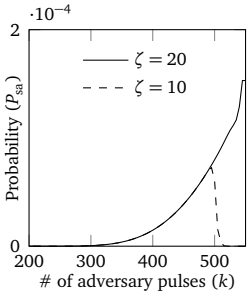
$$p_{\alpha,\beta,r,k}(x,\Gamma) = \sum_{g=0}^{x} \left(p_{\alpha,\beta,r,k,x,\Gamma}(g) \cdot \frac{\binom{x}{g}}{2^x} \right) \tag{5.28}$$

such that

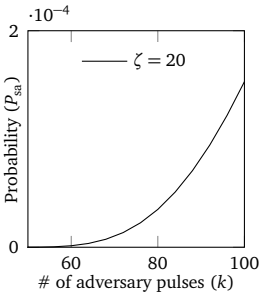
$$p_{\alpha,\beta,r,k,x,\Gamma}(g) = \begin{cases} p_{\alpha,\beta,r,k,x}(g), & k + 2x - 4d \leq \alpha(\zeta - 1) \\ 0, & \text{otherwise} \end{cases} \tag{5.29}$$

Using (5.28), the final adversarial success probability is:

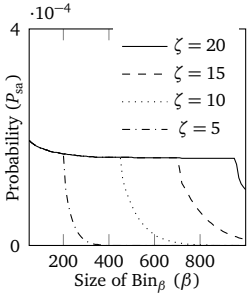
$$P_{\mathrm{sa}}(\alpha,\beta,r,\Gamma,k) = \sum_{x=0}^{\alpha} \left(p_{\alpha,\beta,r,k}(x,\Gamma) \cdot \frac{\binom{\alpha}{x}\binom{\beta}{k-x}}{\binom{\alpha+\beta}{k}} \right) \tag{5.30}$$



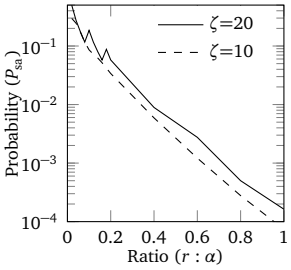
(a) $\beta = 500$; $r = \alpha = 50$.



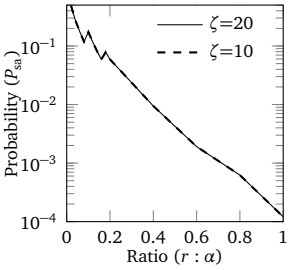
(b) $\beta = 50$; $r = \alpha = 50$.



(c) $r = \alpha = 50$.



(d) $\alpha = 50$ and $\beta = 500$



(e) $\alpha = 50$ and $\beta = 50$

Figure 5.11: Adversarial success probability in (5.30).

Figures 5.11a and 5.11b plot P_{sa} in (5.30). At $\zeta = 20$, Γ is too high to reduce P_{sa}, but the Robust Code Verification check enables the receiver to limit it to $P_{\text{sa}} < 0.16 \times 10^{-3}$. At $\zeta = 10$, P_{sa} stops growing beyond 0.73×10^{-4}, which limits the adversary's pulses to $k = 495$ for its highest success chance.

Figure 5.11c shows the effect of β on P_{sa}; P_{sa} is almost constant with β, at around 0.2×10^{-3}, and only starts dropping when β is sufficiently large so that the aggregate energy after the adversary's pulses exceeds Γ. At a certain point, increasing β no longer helps. For example, at $\zeta = 5$ and $\beta \geq 400$, $P_{sa} \approx 0$. β should thus be set wisely, reflecting the application's sensitivity to distance increases and channel conditions, to avoid increasing transmission lengths unnecessarily.

Symbol length (r)

Figures 5.11d and 5.11e plot P_{sa} against the ratio of $r : \alpha$. As shown, longer symbol length (larger r) is better for security; the best results are achieved when the ratio is 1 ($r = \alpha$).

False positives: noise passing Robust Code Verification

Higher-than-usual noise in the channel might satisfy the Robust Code Verification check. Since the receiver backtracks, it is imperative to calculate the probability, P_{noise}, that noise in the channel satisfies that check. Unlike the adversary's pulses targeted to alter the authentic code, such a candidate trail of noise pulses does not get added to the sender's code because they are at different positions. Without loss of generality, we can separate the noise-intervals in low-energy and high-energy, *e.g.,* across the median of the distribution of N^2. We refer to the number of high-energy intervals as κ. The probability that noise satisfies the Robust Code Verification check is the probability that x of κ pulses fell into Bin_α, by the probability of satisfying the test in that event, $p'_{\alpha,r}(x)$:

$$P_{\text{noise}}(\alpha, \beta, r, \kappa) = \sum_{x=0}^{\alpha} \left(p'_{\alpha,r}(x) \cdot \frac{\binom{\alpha}{x}\binom{\beta}{\kappa-x}}{\binom{\alpha+\beta}{\kappa}} \right) \tag{5.31}$$

where,

$$p'_{\alpha,r}(x) = \sum_{y=0}^{r} \left(\frac{\binom{\alpha-x}{r-y}\binom{x}{y}}{\binom{\alpha}{r}} \cdot \sum_{i=0}^{y} \frac{\binom{\beta-(\kappa-x)}{r-i}\binom{\kappa-x}{i}}{\binom{\alpha}{r}} \right) \tag{5.32}$$

This is the probability that an aggregate of y is chosen from Bin_α, and of $\leq y$ from Bin_β. Since we separate along the median, the expected κ is $(\alpha + \beta)/2$. Figure 5.12 plots P_{noise} against α using (5.31) at $\kappa = (\alpha + \beta)/2$ and $\beta = 100$. Intuitively (and as the chart confirms), $P_{\text{noise}} \longrightarrow 0.5$ as $\alpha \longrightarrow \infty$.

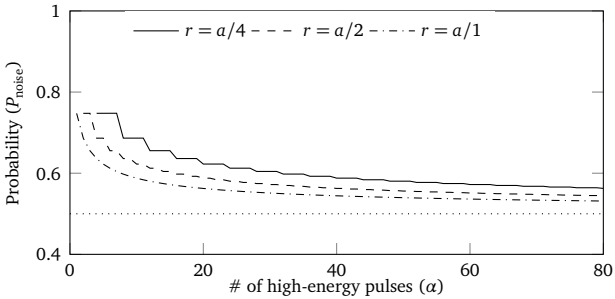


Figure 5.12: Probability that noise passes the Robust Code Verification check, calculated using (5.31); $\kappa = \alpha/2$, $\beta = 100$.

Since a candidate verification code is discarded as noise if the Robust Code Verification check is satisfied with a probability $< P_{\text{noise}}$ (recall: Fig. 5.6), the adversary must have a success probability of at least $1 - P_{\text{noise}}$ to hide the authentic code from the receiver. At $r = \alpha$, $P_{\text{noise}}(80, 100, 80, 40) = 0.53$, and the adversary must thus have a success probability of at least 0.47. As this is much higher than the calculated probabilities in Section 5.2.1, the adversary will not be able to disguise authentic code as noise. The value 0.53 is a lower-bound; in practice P_{noise} should be set ≥ 0.53 depending on applications' requirements and channel conditions.

5.2.2 Validating the Probabilistic Model

The use of prototype implementation using Software Defined Radios (SDRs) and simulations are well-established methods for evaluating wireless systems. Existing SDRs do not support UWB. Therefore, we validate the probabilistic model above with simulations. The channel condition such as noise, multipath effect, and path loss are important factors to consider while designing a wireless system. The IEEE 802.14.4a [118] channel model for different environments is purposefully provided for UWB. The preamble and the verification code are converted into physical layer signals using this model for the outdoor LoS conditions. The model generates the pulse and multipath components to resemble the real-world effect of the channel condition. We assume that upper layers, *e.g.,* Medium Access Control (MAC) layer, could decide on when to perform enlargement detection so that it doesn't interfere with other ranging applications. The simulations account for the noise and

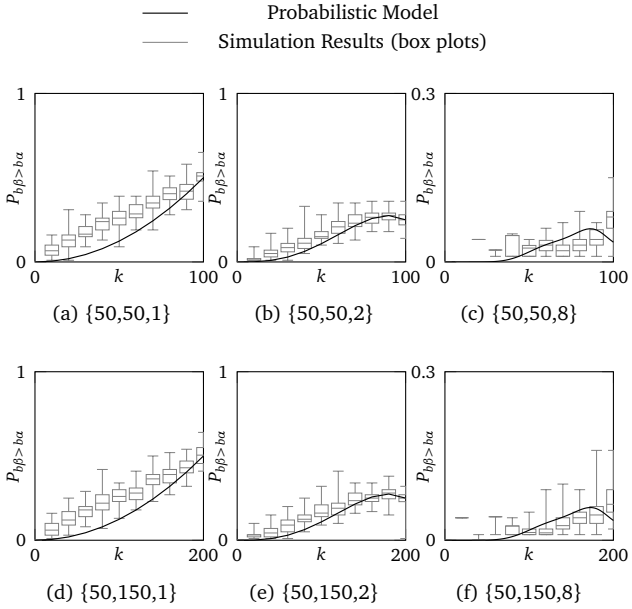


Figure 5.13: Probability of adversary's failure calculated using (5.18), and simulations results validating the probabilistic derivations. Each scenario is run with the $\{\alpha, \beta, r\}$ parameters shown in the charts' individual captions.

interference due to the noise figure of the receiver and multipath components. To verify the simulation setup, we performed a thorough evaluation to cross-check simulation metrics with previous proof-of-concept implementation (UWB-PR implementation in the previous chapter 3)). Each pulse uses 500 MHz bandwidth, and the sampling time between consecutive pulses is 1 μs. Transmission power is limited to -35 dBm/MHz, well under the limits applied by the FCC/ETSI regulations [108]. The energy is further reduced to adapt to path loss model and extra losses (E; *cf.* Fig. 5.7).

An adversary is simulated to inject k signals to annihilate or distort the authentic code, and to replay a delayed and amplified versions of the authentic signals. Similar to our assumptions, the adversary in the simulator is capable of annihilating the pulse and its multipath if the phase is guessed correctly; it doubles the amplitude of the pulse otherwise. The time difference between authentic and delayed signals is $T_D = 200ns$ in the simulations (see Fig. 5.5).

Before demodulation, additive white Gaussian noise (AWGN) is added to the signal. The energy detector receiver is implemented for code verification; it always locks on to the highest peak, *i.e.,* the peak generated by the adversary due to its replay attack. The communication range is considered $100m$, and the backtracking restricted to $660ns$.

The goal of our validation is to (1) confirm the probabilistic model's correctness, and (2) analyze the effect of the parameters abstracted from the model, namely noise and the receiver's ability to reconstruct the signal after long distance propagation. In practice, the latter point can be accounted for by increasing the number of pulses ($n = \alpha + \beta$)—see below.

Validating $P_{b\beta>b\alpha}$. Figure 5.13 shows the validation for $P_{b\beta>b\alpha}$, at a simulated distance between both devices of $d = 10m$. A boxplot is drawn at distinct k, where each scenario is run 10^6 times. The results confirm that abstracting noise from the model does not largely affect its accuracy. Next we show the effect of longer distances on the model.

Validating $P_{\mathbf{sa}}$. Figure 5.14 shows the validation for P_{sa}, at $r = \alpha$ and $P_{noise} = 0.8$. Results are shown for different k, at distances of $10m$ and $100m$. Each scenario is run 10^6 times, and P_{sa} is calculated as the proportion of these where the adversary succeeded to hide the authentic code. Again the results show comparable patterns between the model and simulations. There is a slight horizontal shift at k due to the abstracted noise. In the simulator, Γ is set as in (5.8), which may be a bit too high or low depending on actual noise patterns. In Fig. 5.14a, Γ was relatively low, causing a drop in the simulated P_{sa} at smaller k compared to the model. In Fig. 5.14b, Γ was relatively high, replicating P_{sa} at higher k.

Another difference between simulations and the model manifests with increasing the distance d between both devices. In practice, in UWB, receivers increase their ability to reconstruct the signals (hence, the SNR) by aggregating over more pulses. We noticed that the model provides such comparable probability patters when we decrease α and β in the model proportionally with increasing d in simulations. For example in Fig. 5.14b where $d = 100m$, α and β in the simulator had to be increased from 15 and 158 to 50 and 500 respectively ($\sim$ tripled) to account for the increased distance.

Validating the false positives. We also used simulations to confirm that noise would not be falsely mistaken for authentic code upon proper selection of P_{noise} and Γ. For various distances between $10m$ and $100m$, the probability of a false positive was $\sim 1 \times 10^{-6}$, confirming the noise analysis in Section 5.2.1.

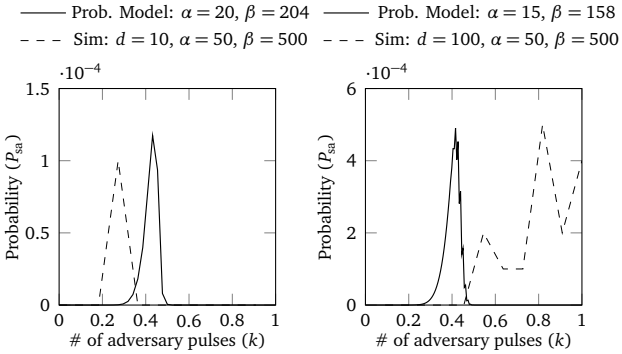


Figure 5.14: The attack is detected when the aggregate energy is between γ and Γ, but $P_{b\beta>b\alpha}$ is more than P_{noise}. The attack is also detected when energy aggregate is more than Γ; $\zeta = 5$.

In conclusion, the simulated probabilities follow comparable patterns with the model, and are in the same range. The model derived herein thus serves as a formal means for evaluating the efficacy and suitability of UWB-ED in practice. The results also show that the channel condition, such as path loss, noise, and interference due to multipath components, does not affect the performance and security of the system. An adversary can increase the noise level, which can increase false positives. High false positives may eventually cause DoS (which the adversary can mount anyway by jamming the channel), but the adversary remains unable to enlarge distances.

5.3 Discussion

Adaptive attacks. An adversary can notice the effect of each of its added pulses on the resultant energy, whether annihilated or amplified. It can then adapt its attack strategy by dynamically deciding k based on the number of pulses it has added/annihilated so far during the transmission. The adversary can then utilize its knowledge of n, α and β in order to, not only decide the optimal value of k statically before the transmission begins, but also adjust their distribution in realtime. This attack does not succeed

because the adversary cannot control the resultant pulse phase. Injecting excessive energy in Bin_β exceeds Γ; injecting in Bin_α does not guarantee annihilation because of the unpredictable phase.

Varying energy levels. To achieve perfect signal annihilation, an adversary uses the same amplitude expected at the receiver. Instead of injecting k pulses each with a constant energy of, *e.g.,* $2\mu W$, the adversary can inject one pulse with an energy of, *e.g.,* $2k\mu W$. If all k pulses fell in Bin_β, the aggregate energy would be the same as when that single high-energy pulse also falls in Bin_β. However, intuitively, the adversary is better off injecting multiple pulses with constant energies for two reasons. First, multiple pulses in Bin_β have higher chances of being selected than a single pulse, thus evading the Robust Code Verification check. Second, for those that fall in Bin_α, any leftover energy after annihilating a pulse, regardless of the phase, will be counted towards the overall aggregate, thus hurting the adversary's cause.

Influencing Γ through distance shortening. Instead of enlarging distances directly, the adversary can first mount a distance-reduction attack to trick the devices into using higher Γ (recall: smaller signal attenuation due to shorter path loss leads to higher Γ calibration). It is thus imperative to complement UWB-ED with a distance-reduction detection [19, 21] with UWB-PR. Devices should alternate between both techniques; *e.g.,* if distances of D_l and D_u are verified using respectively UWB-ED and UWB-PR, it should be concluded that the actual distance, D, is in the range $D_l \leq D \leq D_u$ (D_l is a lower bound, D_u an upper bound).

Influencing the number of pulses, n. An adversary can inject a low stream of noise-like energy, not too high to be detected as jamming. However because Γ is set beforehand, it is not influenced by the adversary. By injecting noise, the adversary actually hurts its own cause as it reduces the amount of energy it can use strategically to prevent code detection.

5.4 Conclusion

In this chapter, we presented UWB-ED—the first known technique to detect distance-enlargement attacks against standard UWB ranging systems. UWB-ED is readily deployable for current off-the-shelf receivers. Evaluation is performed by deriving the probability of adversarial success in mounting distance enlargement attacks. Results show that the verification code structure herein prevents signal annihilation. The code also allows the use

of longer symbol length at the receiver, which is essential to achieve longer distance in the energy-constrained UWB system. Therefore, by using proper integrity checks at the receiver, we can detect traces of the legitimate signal. This design enables the detection of an enlargement attack in the absence of a verification infrastructure.

Part II

OFDM Ranging

Chapter 6
Security Analysis of OFDM-based Ranging Systems

The Orthogonal Frequency Division Multiplexing (OFDM) is widely used in wireless communication due to its ability to effectively utilize the frequency spectrum and its resistance to severe channel conditions. With the increased demand for location information, OFDM-based communication systems are modified to enable distance measurement, the notable examples being WiFi and cellular networks. Although different ranging techniques have been explored for both WiFi and cellular positioning, including received signal strength and multicarrier phase ranging, recent studies indicate adoption of ToF measurement.

WiFi Fine Time Measurement (FTM) was incorporated in IEEE 802.11-2016 (IEEE 802.11mc) [66] and Positioning Reference Signal (PRS) is included in the Location Positioning Protocol for cellular positioning [39, 119]. The WiFi and cellular positioning is expected to enable new, feature-rich, safety- and security-critical applications [120] with benefits to a variety of stakeholders through improved asset and personnel management, geo-fencing with trigger actions (e.g., access control and authentication) [121], network management, navigation [122], and emergency support. Moreover, the IEEE 802.11az standard [123], referred to as WiFi Next Generation Positioning (NGP), is currently under development and expected to largely rely on the fine-timing measurement mechanism introduced in WiFi FTM. Even though 3GPP has put forward a plan to introduce precise positioning into 5G, the current release evaluates potential solutions mainly from the perspective of performance [31, 32, 124].

In this chapter, we analyze the security guarantees of FTM and PRS. The attacks we present can be traced back to the general attack categories. First, these systems do not implement distance bounding protocols to prevent logical layer attacks. An attacker can predict the content of the FTM messages and PRS configurations. Second, ToA estimation is done on the predictable signal structure and transmission time, training fields in WiFi and PRS in cellular. Therefore, an attacker can manipulate ToA estimation to perform both distance reduction and enlargement attacks. Third, using OFDM symbols with the cryptographically generated data does not ensure secure distance measurement; OFDM symbols are few μs long, therefore, allowing the possibility of ED/LC and overshadowing attack.

Furthermore, we identify that an attacker can manipulate reference signals or preamble to prevent legitimate symbols detection in order to mount distance enlargement attacks.

The structure of this chapter is as follows. We give background of the FTM protocol and analyze its security against different distance manipulation attacks in Section 6.1. In section 6.2 we expose security vulnerabilities of PRS. We show that there exist novel attacks that have not been discussed so far and only arise due to the use of coherent receiver design in Section 6.3. We discuss fundamental limitations of these systems is Section 6.4, and concludes our findings in Section 6.5.

6.1 WiFi Fine Timing Measurement

FTM enables stations to determine their physical distance by measuring the round-trip time of frames exchanged between them. For example, mobile devices can use FTM to determine their distances from several access points (APs) and estimate their precise position. A WiFi FTM distance measurement session consists of three phases: (i) negotiation, (ii) measurement exchange, and (iii) termination phase [125]. An overview of two stations (initiator and responder) executing an FTM session is shown in Figure 6.1. Typically, the initiator is a mobile device that wants to estimate its distance or location, and the responder is an access point. The standard allows a WiFi FTM supported station to act as an initiator or a responder. The initiator starts the negotiation phase by transmitting a request frame, this frame includes configuration parameters and vendor-specific information elements. The responder, often configured as an access point, responds with a status code indicating success or failure for the requested parameters. The measurement exchange begins if the status code indicates success. The stations timestamp every transmission and reception during the measurement exchange. Upon receipt of response frames, the initiator calculates the round-trip times. The average round-trip time is calculated using the following equation

$$RTT = \frac{1}{n}\sum_{x=1}^{n}((t4_x - t1_x) - (t3_x - t2_x)) \tag{6.1}$$

where n is the total number of distance measurements. From the calculated RTT value and knowing that radio signals travel at the speed of light, the initiator derives the distance. For the initiator to track which timestamps correspond to its measurements and account for re-transmissions, the

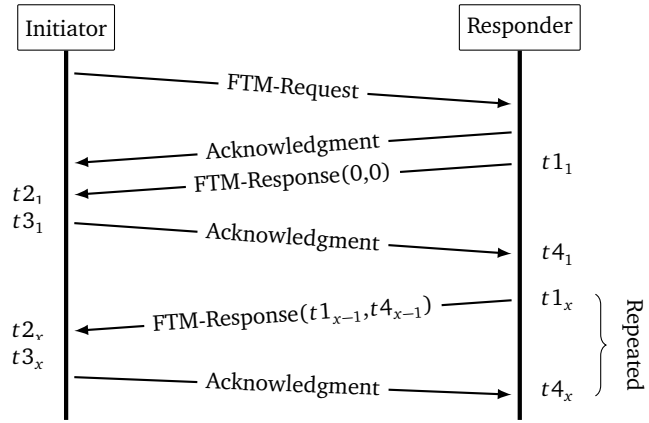


Figure 6.1: Fine Timing Measurement session with ASAP=1, and x-number of measurements per burst.

	1	1	1	1	6	6	4	4
MAC Header	Category	Action	Token	FU Token	FTM ToD	FTM ToA	Errors	FCS

Figure 6.2: Simplified construction of a WiFi Fine Timing Measurement (FTM) Response frame.

responder includes dialog tokens in its response frames. The first response frame contains a non-zero dialog token and is increased sequentially over consecutive response frames within the session—a simplified construction of the response frame given in Figure 6.2. The follow-up dialog token is set to the dialog token of the previous response frame. Finally, the session is terminated after a negotiated number of measurement exchanges are completed. The initiator and responder can terminate the session by requesting a new session with modified configuration parameters and by setting dialog token to zero.

Support for WiFi FTM was introduced in Android 9 [126]. Also, Google provided an example WiFiRTTScan application for developers to build positioning, navigation, and context-aware applications. The WiFi Alliance lists certified devices [127], and includes manufacturers like Qualcomm, Broadcom, and Intel.

Layer	Attack Type	Effect	Resolution
Logical	Inject Response	●	1 ps
Physical	Replay Overshadow	●	1 ps
	Earlier Path Injection	◐	1 ps

Table 6.1: FTM: Overview of various distance reduction (◐) and enlargement (◑) attack types, with its resolution.

Physical-Layer Configuration One of the most important physical-layer parameters directly impacting ranging precision is the signal bandwidth. Though not required by the specification, a station is likely to use IEEE 802.11ac due to its support for wide bandwidths (upto 160 MHz), implying the usage of Orthogonal Frequency-Division Multiplexing (OFDM), with Binary Phase Shift Keying (BPSK) modulation, and a long Guard Interval (GI). The initiator requests its desired configuration in the FTM parameters field and is confirmed by the responder in its first response frame. If the responder agrees to a wider bandwidth, it switches to the respective channel and bandwidth before transmitting its first response frame. An initiator can learn about the supported capabilities by inspecting the beacon frame transmitted by the responder, e.g., Very High Throughput (VHT) field in IEEE 802.11ac.

Time-of-arrival Estimation: The header's Training Fields (TF) are used for gain control, packet detection, and clock synchronization. VHT-LTF field is the preferred choice for ToA estimation in IEEE 802.11ac based FTM receiver designs [128]. However, a receiver can combine samples from multiple fields for ToA estimation. The receiver performs cross-correlation between received and expected training field sequence to estimate Channel Impulse Response (CIR) for ToA estimation, *i.e.,* leading edge detection.

6.1.1 Attacks on WiFi FTM Ranging

Table 6.1 lists a subset of attacks possible on the FTM, with the layer manipulated, and whether it allows for distance reduction or enlargement. Additionally, it lists the resolution, that is, the granularity with which a distance modification can be introduced. Obviously, the attacker has complete knowledge of the IEEE 802.11-2016 [66] measurement protocol. WiFi FTM was designed to be seamless, i.e., stations or devices need not associate themselves to an access point to execute the ranging protocol, and therefore lacks any form of authentication or encryption. Some of these

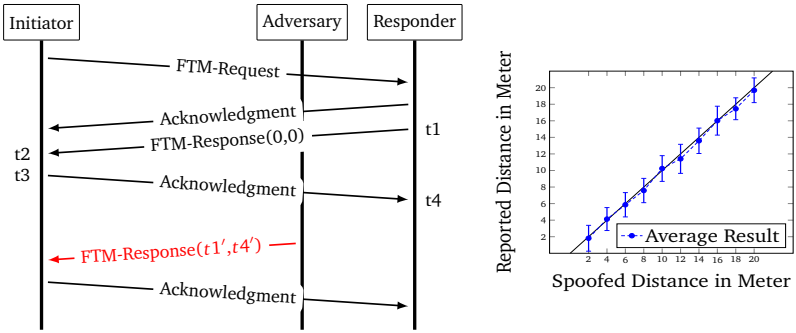


Figure 6.3: An adversary can reduce or enlarge the measured distance by spoofing response frames with modified round-trip timestamps ($t1'$ and $t4'$) with meter-level precision. Results are shown for Pixel 4 XL as initiator and WILD AP as responder.

attacks can be carried out using off-the-shelf WiFi dongles by changing transmission parameters such as MAC address and content for the payload.

(A) Spoofing FTM Responses

An adversary can inject spoofed FTM-response frames and alter the measured distance to *any* attacker chosen value. Figure 6.3 shows a high-level overview of the attack. The FTM-response frame contains the previous response and acknowledgment frames' time of departure t_1 and time of arrival t_4 respectively, and are used in estimating the round-trip time. An adversary can modify these timestamps, thereby affecting the measured distance. Since this transmission is seldomly encrypted, it is straightforward to introduce fake distance measurements; for example, an adversary can capture timestamps from a previous measurement round, modify timestamp t_4, and replay the results. The granularity by which the attacker can manipulate the distance depends on the attacker's ability to determine the processing time. Few industry patent applications propose secure out-of-band channels to share unique dialog tokens or nonces [129] or share timestamps in protected range reports [130], but they are not implemented on the existing systems.

Experimental results: Figure 6.3 presents results for spoofing FTM response when using Google Pixel 4 XL as an initiator and Compulab WILD as responder. The results show that an external attacker can spoof the

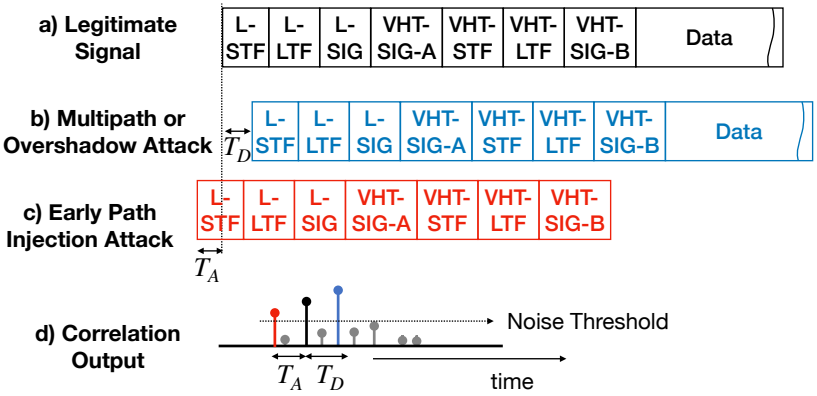


Figure 6.4: Physical-layer attacks against WiFi FTM, manipulating time-of-arrival of IEEE 802.11ac frames.

response frame with a high acceptance rate and meter-level accuracy, and the inaccuracy of the committed distance is no more 5 *ns* (1.50 *m*).

(B) Replay Overshadow Attack

WiFi FTM's ranging accuracy in multipath scenarios can be off up to 20 m [131]. A measured distance more than the actual distance implies that the receiver has used multipath for ToA estimation. However, a measured distance less than the actual distance indicates that an earlier side peak detected during backsearch is used for the distance measurement. The physical layer attacks exploit FTM's physical-layer representation and receiver design; the attack signal overlaps with the legitimate signal to manipulate the signals' arrival time.

An attacker can achieve distance enlargement by replaying the legitimate frame with a higher power after a delay of T_D (Figure 6.4b). Both the attacker and legitimate signals overlap, and the receiver cannot distinguish between their arrival time, as shown in Figure 6.5. Even though the initial samples collected during time T_D are unaffected by the attack signal, they are not sufficient to perform ToA estimation and therefore are discarded as noise. The receiver performs cross-correlation or CIR estimation using the entire LTF sequence for ToA estimation. The attack succeeds if the attack signal's correlation peak is the highest, and the legitimate peak is not detected during backsearch, either because the delay T_D is more than the back-search window or the power of the legitimate peak is below the noise threshold.

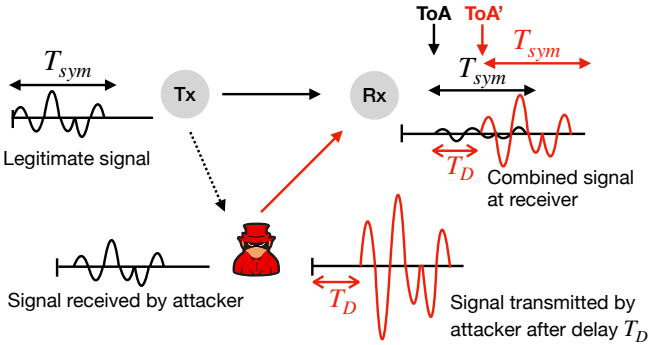


Figure 6.5: Distance enlargement: symbol overshadow attack.

The receiver also detects correct data for the attacker's peak; the attack signal is a copy of the legitimate signal. This attack type cannot be prevented even with cryptographic protection of the payload data, as the fundamental problem is the usage of OFDM symbols. We note that the attacker can cause significant distance enlargement with a delay $T_D \ll T_{sym}$. FTM uses long OFDM symbols (symbol duration $T_{sym} = 4\ \mu s$) to represent both header and payload data at the physical layer, the overshadowing signal arriving after a delay of $T_D = 0.16 \mu s$ (4% percent of symbol length) achieves distance enlargement of $\approx 48\ m$. By increasing the value of T_D, the attacker can achieve several hundred meters of distance enlargement.

Injecting Spoofed Acknowledgments: A special case of an overshadow attack is when the attacker takes advantage of the acknowledgment's static data. An attacker can transmit a spoofed acknowledgment earlier or later and with higher power than the legitimate frame to modify the round-trip time estimate and, as a result, manipulate the distance. The attack succeeds as the receiver *locks on* to the higher power peak or one of its side peaks for ToF estimation since the LTF sequence of both legitimate and attack signals overlap.

Experimental results: To access sample-level information, we perform a MATLAB simulation. We evaluate the overshadowing attack on the BPSK modulation OFDM symbol, transmitted at the typical LoS channel at signal-to-noise-ratio (SNR) of 20 dB. As shown in Figure 6.6a, the attack's overshadowed OFDM symbols have no bit error if its power is three times ($\approx 4.8\ dB$) higher than the legitimate signal. The attack signal hides the

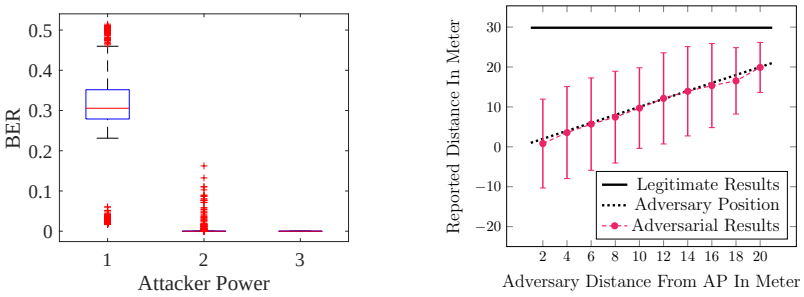


Figure 6.6: For an overshadow attack, a weak power level leads to bit errors (a). Spoofing acknowledgments proves successful for a distance reduction attack (b).

legitimate signal to prevent its detection; it does not need to jam or saturate the receiver. If the attack signal has enough power, the back-search window does not have any bearing on this attack - the attacker can choose the delay T_D to be smaller or higher than the back-search window.

An attacker can spoof acknowledgment frames since it contains static data, and the MAC address of the AP is known in advance. Figure 6.6b shows spoofing results when using Compulab WILD as the initiator and Google Nest as the responder. In the absence of an adversary, the initiator reports a distance of $\sim 30\ m$. As the adversary starts acknowledging frames and moves towards the AP, the reported distance decreases accordingly. These findings highlight a fundamental protocol flaw, whereby an adversary capable of acknowledging frames can effortlessly reduce the distance.

(C) Earlier Path Injection Attack

The reported distance measurement may be shorter than the actual distance, with its error more than the imprecision of the system [131]. This is a side effect of the backsearch algorithm, i.e., the receiver uses a correlation output's side peak for ToA estimation. These frames report correct data, suggesting that the receiver is using the strongest peak's arrival time for packet detection and data recovery; using a lower power side peak's arrival time results in incorrect data. These results suggest that payload detection and ToA estimation in FTM are non-binding; the receiver uses the highest correlation peak for data detection and an earlier peak for the ToA estimate.

The backsearch is critical for accurate distance measurement; otherwise, FTM cannot perform under multipath and NLoS scenarios.

An attacker can exploit the receiver design to perform a distance reduction attack (Figure 6.4c), i.e., insert a peak within the backsearch window. The preamble is fixed and, therefore, can be replayed or transmitted early. The attacker transmits only the header part of the frame and carefully controls its arrival time and power. First, the attack signal should arrive T_A time earlier than the legitimate frame at the receiver, and T_A should be smaller than the backsearch window. The signal will not be used for ToA estimation if it arrives too early or late. The attacker should know the distance between the devices and use benchmarking to estimate the transmission time of acknowledgment frames. This information is sufficient to predict the arrival time of the legitimate acknowledgment frame, and an attacker can then transmit the attack signal accordingly. Second, the attacker should control the attack signal's power, as too low or too high power makes it ineffective. If the power is higher than the legitimate signal, the receiver *locks on* to the attacker's peak for packet detection and ranging fails due to incorrect data. If the power is below the noise threshold, the signal is not detectable during the backsearch. Therefore, the attack signal's power should be higher than the noise threshold but lower than the legitimate signal. Though a receiver can choose a noise threshold in advance, the legitimate signal's received signal strength varies depending on the channel condition. Several studies [132] have shown the feasibility of predicting received signal strength at a receiver location, in the context of channel-based key establishment.

Receivers generally use the same training sequence for ToA and channel estimation. The attacker's attempt to introduce an earlier peak can compromise channel estimation, preventing data detection. We consider the attack successful only when the following conditions are satisfied - (i) peak is introduced within the backsearch window, (ii) the peak's power is between the noise threshold and the highest peak, and (iii) the data is detected correctly. FTM's current physical layer cannot prevent an earlier path injection attack as the receiver optimizes both ToA estimation and data detection.

Experimental results: We used simulations to evaluate 802.11ac VHT waveform with a TGac fading channel (Model-B) [133]. We use VHT-LTF training sequences for ToF estimation and a back-search window of 100 ns at SNR of 20 dB. Figure 6.7a shows power distribution of side peaks within the back-search window of the highest peak. The receiver has to

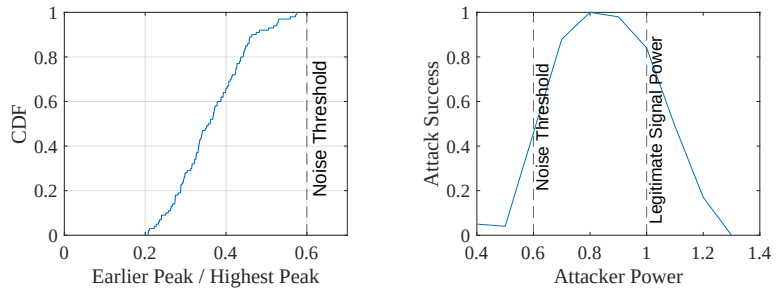


Figure 6.7: Receivers use a noise threshold higher than any side peaks (a). An earlier path injection requires the injected peak's power to be within a threshold (b).

choose the noise threshold's value to differentiate the direct path signal from the side peaks based on power distribution. In this particular receiver design, setting the noise threshold to 0.6 minimizes the false positives. Using a lesser value trigger the detection of side peaks as an earlier path, and setting a higher value misses the direct path; in both conditions, the distance estimation is incorrect.

In this particular receiver design, an earlier path injection is successful if an attacker injects a signal (i.e., frame header) within the back-search window, with its power under certain thresholds. Figure 6.7b shows the success probability for different signal strengths, assuming the signal arrives within the back-search window. A low power signal is discarded as noise, and a higher power distorts channel estimation and prevents data detection. The attack is successful when an earlier peak injected by the attacker is used for distance estimation, and the legitimate signal is used for data recovery.

ED/LC attack on OFDM Symbols: Even if a receiver checks for consistency in the estimated arrival on training sequence and arrival time of data symbols, an attacker can still perform ED/LC attack to advance the arrival time of the symbols. For example, an attacker can exploit the repetitive nature of the cyclic prefix and BPSK modulated OFDM symbols. Such attacks have already been demonstrated [90] and can be considered as a form of late commit attack.

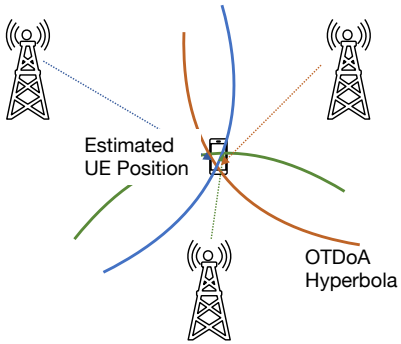


Figure 6.8: User Equipment (UE) receives PRS from the nearby base stations and estimates relative differences between arrival times.

6.2 LTE/5G Positioning Reference Signal

The positioning information in LTE is mainly provided by GNSS (*Global Navigation Satellite System*), which is reasonably accurate outdoors where line-of-sight with a sufficient number of satellites is guaranteed. However, due to the limited availability of satellite signals in city centers and inside, LTE implements additional ways of determining user equipment (UE) position under LTE Positioning Protocol (LPP). The LPP protocol supports Enhanced Cell Identity (E-CID), Assisted GNSS (A-GNSS), Observed Time Difference of Arrival (OTDOA), and hybrid localization (A-GNSS + OTDOA). The current standards recommend OTDOA with the Positioning Reference Signals (PRS) that support downlink-based positioning methods. The PRS is specifically designed to deliver the highest possible levels of accuracy, coverage, and interference avoidance and suppression [134, 39]. These signals are designed to measure accurate ToA of the weak signal originating from distant cells even in the presence of a stronger signal from serving and closer cells. The position is calculated by observing the ToA of the PRS signal originated from the serving cell and other neighboring cells as shown in Figure 6.8. The ToA is estimated by correlating the received signal with a locally generated reference signal. The PRS is designed to enable broadcast-based service and does not convey any higher layer information. Information needed for the local reference generation, such as physical-layer cell identity, number of resource blocks allocated to PRS, subframe number, and other optional fields, is available to each user. Some of these parameters are communicated in advance by LPP protocol,

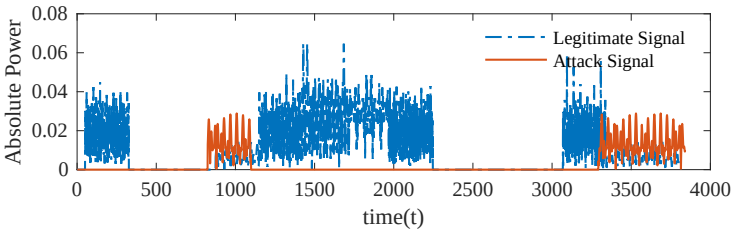


Figure 6.9: PRS arrival time manipulation: legitimate signal (in blue) contain PRS signal and information needed for PRS detection, such as cell identity. The attacker is sending PRS signal (in blue) with the higher power in advance.

while others are contained within the subframe containing PRS. Any receiver capable of decoding LPP protocol can create a local copy of the expected PRS signal and correlate it with the received signal to estimate its arrival time [135, 136]. The new release of the 5G standard has enhanced LTE positioning with the PRS in downlink and the sounding reference signal (SRS) in uplink. The PRS is still the main reference signal supporting downlink-based positioning methods.

Manipulating PRS ToA: The data transmitted as part of the LPP protocol or in the subframe is intended for all UE requesting location measurement. Therefore, an attacker can use a UE or an open platform like srsLTE to obtain this information. After acquiring this information, an attacker has all the information needed to generate a local copy of the PRS signal. Therefore, an attacker can overshadow the legitimate signal to manipulate ToA estimation. As shown in Figure 6.9, an attacker can advance the arrival time of the PRS. Similarly, an attacker can send it after a delay for distance enlargement. This attack is similar to the overshadowing acknowledgment packets of the WiFi FTM shown in the previous section.

Experimental results: Mobile phone providers have recently started implementing PRS [137], and it is yet not supported by open-source implementations such as srsLTE [138], Open Air Interface [139], and base stations in our region. We analyze attacks on the PRS using MATLAB LTE toolbox and software-defined radios USRPs. Yang *et al.* [140] showed the possibility of performing the overshadowing attack on the LTE systems, an attacker in practice can use a similar approach to synchronize attack PRS transmission with the legitimate PRS transmission.

Attack/Legitimate [dB]	**0**	**3**	**6**	**9**	**12**	**15**
$T_A = 5\ \mu s$	0	0.93	1	1	1	0.3
$T_A = 15\ \mu s$	0	0.89	1	0.99	1	0.21
$T_D = 5\ \mu s$	0	1	1	1	1	0.11
$T_D = 15\ \mu s$	0.01	0.9	1	1	1	0.2

Table 6.2: PRS time-of-arrival manipulation success rate.

To realize the PRS enabled ToA estimation, we generated a resource grid containing Primary and Secondary Synchronization signals (PSS, SSS), cell-specific reference signals, and PRS using the example provided by MATLAB [141]. We transmit this signal using USRP at the sampling rate of 3.84 MHz, using the Reference Measured Channel (RMC) 5 configuration. Another USRP receives the signal to acquire cell-related information, such as cell identity, and perform ToA estimation.

The attacker has all the necessary information for PRS generation and transmits the PRS signal in advance by T_A or delay by T_D duration. At the receiver, we check the reference signal received quality (RSRQ) and the cell-related data's correctness. The attack is considered successful if both RSRQ and cell data are correct and the estimated ToA matches the time offset intended by the attacker. The probability of attack success is shown in Table 6.2. We show that the attacker can manipulate the arrival time estimation without manipulating other reference signals or data required for cell detection. The probability of attack success reduces if an attacker uses very low or high transmit power, as the received signal does not fit the RSRQ check. The attack we present here achieves a very high success rate and represents the best-case scenario.

In real settings, to position a user device at the intended location, the attacker must repeat this attack for all base stations in the communication range. An attacker would also need to select the value of T_A and T_D carefully. This attack scenario is similar to GPS spoofing, where an attacker chooses delay for each satellite [56]. In chapter 7, we propose a design that can be used as an alternative to using PRS in the 5G systems.

6.3 Carrier Frequency Offset Attack

In this section, we introduce a novel *carrier frequency offset attack*. This attack can be viewed as a special case of distance enlargement - an attacker takes advantage of the predictable reference signals and coherent receiver design. In a ToF ranging system, it is crucial that the transmitter

and the receiver tune to the same carrier frequency for secure and precise ToF estimation. This assumption also holds for any wireless system requiring integrity of the signal, see, e.g., [73, 74]. Even though the carrier frequency f_c can be precisely and secretly communicated to the devices, due to the mismatch in the transmitter and the receiver frequency oscillator [142], the devices will experience Carrier Frequency Offset (CFO) and phase offset. The offset is typically corrected with the help of reference signals, *e.g.,* the preamble in UWB-HRP [99], training sequences in the WiFi [128], and phase tracking reference signals and synchronization signals in 5G [143, 144]. A receiver can estimate CFO using the expected and received reference signal and correct it. The presence of offset results in inter-carrier interference, signal attenuation, and phase rotation. The incorrect offset estimation in conventional communication systems leads to a high symbol error rate and potentially a denial of service due to the imbalance in the in-phase and quadrature components of the signal's power distribution. In a ranging system, an incorrect offset estimation results in a time-shift of received signals affecting the measured distance directly. Unfortunately, the use of fixed reference signals for offset estimation also makes coherent receivers, including 5G, vulnerable to distance modification attacks. Instead of correcting the offset, an attacker can use reference signals to increase their offset. The reference signal is predictable; an attacker can modify, annihilate, or delay it. We show an attack on the ranging system by using frequency offset manipulation.

As shown in Figure 6.10, distance manipulation happens in two steps. First, an attacker performs the overshadowing attack on the reference signal, which are also OFDM symbols. The attacker's hardware oscillator error e_a' is different from the oscillator at the legitimate transmitter e_a, and the attacker signal also has a higher power. The attacker's high power signal affects the frequency offset (Δ) estimation at the receiver – the new estimated offset (Δ') is incorrect to recover legitimate transmission. In the second step, the attacker replays the legitimate signal with a delay T_D calculated based on the oscillator error e_a'. As the receiver is tuned to an incorrect offset Δ', it *locks on* to the attacker's replayed signal and decodes the correct data but with a time offset, thereby increasing the measured distance. The receiver discards the legitimate signal as noise (strong multipath) as it does not provide correct data even though it has finite energy. In Figure 6.10b, the attack is shown using short symbols to emphasize that short symbols are also vulnerable to the offset manipulation attack. This system only affects coherent receiver designs, and issues occurring due to the minor carrier

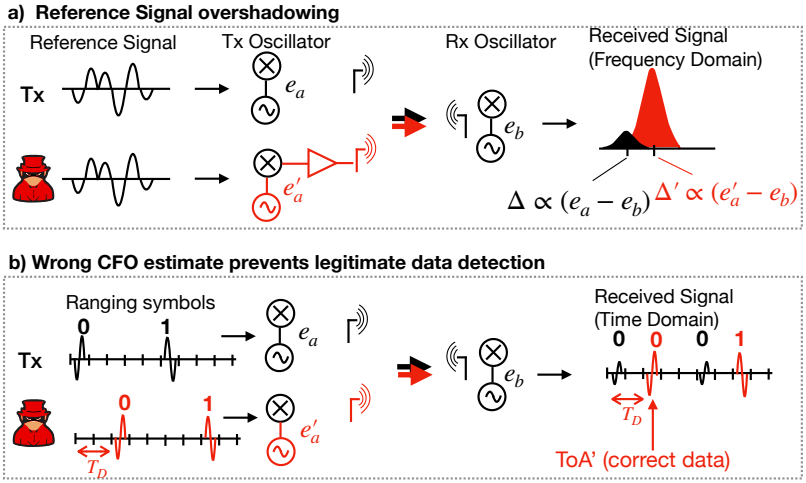


Figure 6.10: Distance enlargement by manipulating frequency offset estimation.

frequency mismatch are not relevant to energy detector receiver designs (UWB-PR and UWB-ED are therefore not vulnerable to CFO mismatch). Later, in chapter 7, we discuss this attack in the context of the secure design we propose and show that offset mismatch of 10 KHz is sufficient to prevent data detection [1].

6.4 Discussion

Improving Logical Layer The analysis of the FTM and PRS shows that they are not designed to prevent logical layer attacks. An attacker can impersonate both FTM response and acknowledgment frames - the only frames used in the time-sensitive part of the ranging protocol. An attacker can manipulate the response frame's payload, which contains the value of the estimated ToA, and therefore control distance estimation. On the other hand, the acknowledgment frame does not contain any payload. The LTE/5G assigns a PRS sequence to the base station, and the base station repeatedly transmits this sequence to enable a broadcast positioning system. In both WiFi and LTE/5G, the payload and reference signal prediction can be avoided by cryptographically securing them, thereby preventing

[1] Transceivers operating at 4 GHz and a clock error of 10 ppm expect carrier frequency offset up to ±80 KHz

logical layer attacks. The following improvement will help improve the security. First, the payload/reference signal should be unpredictable for an attacker. For example, payload should be encrypted and PRS sequence should be chosen randomly from different configurations. Second, the transmission time of the acknowledgment frame and PRS signal should be chosen randomly. It will prevent benchmarking of WiFi SoCs and will render replayed sessions and responses inaccurate. The attacker would have uncertainty in the transmission time of the PRS, and therefore need a more involved attack to align transmission of the attack signal with the legitimate PRS signal.

Physical-Layer Limitations Since cryptographic protection of data does not prevent physical-layer attacks, a system's security depends on its radio receiver design and implementation. FTM and PRS remain fundamentally vulnerable in scenarios where multipath cannot be estimated securely and accurately. For example, overshadow, early path injection, and carrier frequency offset attacks take advantage of the receiver's inability to estimate the channel correctly and securely. First, due to the longer symbol duration, it is hard to determine the actual arrival time of the signal and differentiate multipath from the attack signal. For example, suppose a receiver binds the training sequence's arrival time with data's arrival time in the WiFi FTM. This receiver will observe high misdetection when the direct path signal is hidden under the multipath. Second, the coherent receiver needs to resolve each sample's phase, and an attacker can compromise it to prevent detection of the legitimate direct path signal. In the next chapter, we present an approach to construct shortened OFDM symbols using data bits generated by distance bounding protocols and integrity checks at the receiver to prevent physical layer distance manipulation attacks. This design can be considered as a secure candidate for a sufficiently wideband WiFi and 5G ranging systems.

6.5 Conclusion

In this chapter, we analyzed the possibility of logical and physical layer attacks on the OFDM-based ToF ranging systems - WiFi FTM and LTE/5G PRS. We show that an attacker can use off-the-shelf hardware to perform both distance reduction and enlargement attacks. This analysis exposes the fundamental problem of using OFDM symbols for ranging, and the attacks are easier to mount due to longer symbol duration. We also propose a novel carrier frequency attack - this indirect attack manipulates CFO estimation to

prevent legitimate data detection in order to mount distance enlargement attacks. This analysis shows that WiFi and cellular positioning cannot be secured using cryptographic protection at the logical layer, exposing the necessity of a secure physical layer design.

Chapter 7
V-Range: Enabling Secure Ranging in 5G Wireless Networks

As shown by the security analysis of 5G/LTE PRS, the existing cellular positioning can not be trusted. 5G is expected to offer high-precision indoor and outdoor location and positioning services. 3GPP, the standards organization responsible for developing the 5G New Radio (5G-NR) architecture, intends to leverage the 5G network architecture and high bandwidth to enable state-of-the-art positioning techniques [29, 145, 134]. The availability of larger bandwidth in millimeter-wave frequencies makes 5G a perfect fit for high-accuracy positioning. Several applications, including asset tracking, autonomous navigation, supply chains in the manufacturing industry, *etc.*, are expected to benefit from absolute and relative positioning [146, 147].

We note that for several applications that 5G-NR targets, popular positioning systems such as LIDAR or GPS are either unavailable or unreliable (e.g., LIDAR in bad weather or GPS in an indoor setting). In scenarios like vehicle-to-everything (V2X) communication, we expect 5G-NR positioning to complement existing technologies *e.g.,* applications will fuse data from GPS, LIDAR, and 5G-NR to minimize position uncertainty [148, 149, 150]. It is worth pointing out that attacker can manipulate both LIDAR [151, 152, 153] and GPS [52, 56]. 5G's precise distance measurements will increase every individual road user's contextual awareness and improve road safety as a whole [154, 155, 156]. Additionally, the computed location information is expected to augment services running on top of the 5G infrastructure and target applications (e.g., localization during emergency calls) within 5G's architecture itself. 3GPP and other standardization bodies are thus actively working with industry and academic partners to define 5G positioning systems' performance requirements. Even though 3GPP has put forward a plan to introduce positioning into 5G, the current release evaluates potential solutions mainly from the perspective of performance [31, 157, 32]. Many use cases for 5G positioning reside in a security- or safety-critical context. Therefore, it is crucial to devise a localization and ranging mechanism that is both precise and secure, i.e., it must not be subverted by adversarial interference.

In this work, we design the first secure ranging system for 5G-NR radio architecture and demonstrate that our system is secure against distance reduction and enlargement attacks. We enumerate the challenges that need to be addressed to enable secure positioning in 5G. Our solution can be integrated into the 5G-NR radio architecture and does not affect or deviate from existing standards and proposals. We build a proof-of-concept for sub-6GHz and mm-wave modes of 5G communication and evaluate their performance and security guarantees. Our V-Range system uses shortened OFDM symbols in which energy is aggregated over a short time period. A V-Range receiver can ensure that distance estimation is correct by applying proper data and sample-level integrity checks. The short effective symbol length and the added signal and data integrity checks guarantee resilience against all known distance reduction and enlargement attacks. Our security analysis confirms that V-Range constitutes a highly secure ranging system. The success probability of a reduction attack is 10^{-7} and an enlargement attack is $\approx 10^{-5}$ for a 4-QAM modulation scheme. The probabilities are computed *per* ranging operation and consider the cases where an attacker can modify the measurement by more than the imprecision of the system, i.e., 3 m for sub-6GHz and 60 cm for mm-wave band. We also show that V-Range can perform a (two-way) time of flight measurement in 83 μs, enabling a high refresh rate and high temporal resolution for high-density application scenarios.

7.1 Background

7.1.1 5G New Radio (5G-NR)

5G has a dynamic Time Division Duplex (TDD) frame structure as shown in Figure 7.1; slots can be assigned flexibly to uplink or downlink channel. Every symbol in a slot can also be configured in a variety of ways based on the application. For device-to-device communication (e.g., vehicle-to-vehicle communication), or in the absence of a base station , the device initiating the communication within a slot is considered to transmit on the downlink channel and any other (responding) device on the uplink channel. This allows two devices to use the same slot [158].

Every slot consists of 14 OFDM symbols. However, 5G-NR standard allows accommodating more symbols using slot aggregation. The OFDM is a digital multi-carrier modulation scheme that uses closely-spaced orthogonal subcarriers to transmit data in parallel. The symbol length (T_{sym}) depends on the bandwidth of the subcarriers, and not on the total bandwidth of the system. For example, an OFDM symbol in 5G-NR can have a minimum

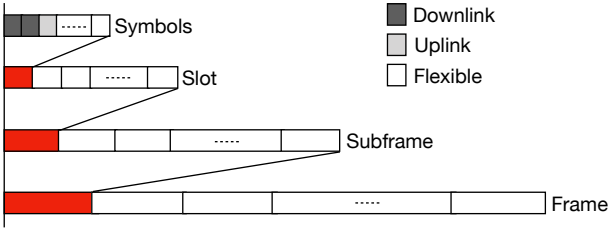


Figure 7.1: Dynamic frame structure of 5G. A frame is divided into subframes and slots. Slots are used for the transmission of symbols and can be allocated for uplink or downlink.

Subcarrier Bandwidth (kHz)	**Max Bandwidth** (MHz)	**Sampling Rate** (Msps)	**Symbol Length** (μs)
15	50	61.44	66.67
30	100	122.88	33.33
60	200	245.76	16.67
120	400	491.52	8.33
240	400	491.52	4.17
480	400	491.52	2.08

Table 7.1: 5G Numerology. Max system bandwidth and sampling rate based on subcarrier bandwidth.

symbol length of 2.08 μs (at subcarrier bandwidth of 480 kHz), irrespective of the total bandwidth allocated to the system. Devices operating in sub-6GHz frequency bands support subcarrier spacing of up to 60 kHz, and mm-wave devices support much higher subcarrier bandwidth, up to 480 kHz. The different configurations are listed in Table 7.1.

7.1.2 Positioning with 5G-NR

Several public and private companies, including hardware and equipment manufacturers, space agencies, and mobile network operators, are pushing for the delivery of higher accuracy and precision by cellular location services to enable a new generation of commercially motivated location-based services. Cellular positioning has found its application in multiple areas, including asset tracking, smart cities, healthcare, UAVs, and augmented reality. The existing approaches are insufficient to achieve the accuracy and reliability demanded in these use cases. As a result, 3GPP is taking a fresh look at the application space and performance requirements for cellular positioning. Compared to earlier standards, 5G-NR's flexible design, wider bandwidth, mm-wave frequency bands,

massive MIMO capabilities make it ideal for realizing high precision, low-latency ranging systems [33, 159, 31]. 3GPP is already exploring the feasibility of using different distance measurement techniques such as round trip time, time of arrival, angle of arrival, and carrier-phase based techniques [145, 30, 160, 144] and designing new signals to support various ranging techniques. In the transportation sector, ranging systems are expected to support traffic management and collision prevention with several field tests already ongoing to explore capabilities of 5G enabled vehicle-to-everything communication and ranging [155]. The street-level mm-wave base stations are expected to enable accurate positioning for autonomous driving and drone maneuver [134, 33].

7.2 V-Range – Secure Ranging in 5G

The security analysis in the previous chapter showed that OFDM-based ranging systems, including 5G, are vulnerable to physical layer attacks such as ED/LC, overshadowing, and carrier frequency offset attacks. There are several fundamental requirements for building a secure 5G-NR ranging system. First, the information transmitted as part of a ranging operation needs to be encapsulated within short symbols. This significantly reduces the effects of distance manipulation as symbol length limits the theoretical time a signal can be advanced/delayed by an adversary. However, the shortest symbol duration available in 5G-NR is around 2 μs and can result in several hundred meters of distance manipulation. In other words, it is essential to limit the symbol duration significantly to prevent distance manipulation attacks.

To realize a secure ranging system, we also need a secure verification process at the receiver, which cannot be compromised directly (*e.g.,* ED/LC) or indirectly (*e.g.,* predictable reference signals for offset correction). The receiver needs to implement integrity checks at both the physical and data levels to guarantee unmodified delivery of time-critical messages. These checks need to be carefully engineered, guaranteeing security against a variety of communication channel conditions without raising a number of false alarms [94]. The designed system should ensure to the maximum extent possible that the legitimate signal is not discarded as noise since this leads to the enlargement attack success. In other words, we need integrity and sanity checks that account for anomalies that can result from the legitimate communication channel conditions while detecting all known distance manipulation attacks.

7.2.1 System Overview

The V-Range is a two-way ranging system used to establish distance between the user equipment and base station, or two user equipment. We assume that the systems use logical-layer algorithms and protocols (e.g., distance bounding protocols) to generate the challenges and responses to prevent logical layer attacks. The 5G's flexible slot length allows the transmission of challenge and response of a flexible length. We assume that the ranging devices negotiate the transmission schedules and their slot assignment as part of the standard medium access, *i.e.,* transmitter initiates transmission of the ranging signal at a pre-negotiated time. The receiver needs to initiate the signal reception a bit earlier than the pre-negotiated time. This is needed to account for the reference clock mismatch between the two devices. The devices agree in advance which numerology and modulation are to be used during the ranging operation.

Standard 5G symbols transmitted using OFDM are long (*i.e.,* few μs) and, therefore, are vulnerable to distance reduction and enlargement attack. The V-Range transmitter compresses the effective OFDM symbol length by transmitting the same data in all subcarriers; this is in contrast to conventional OFDM, in which each of the subcarriers can carry different data. The result is the aggregation of symbol energy over a short time period (*i.e.,* few ns), making it harder for an attacker to perform early-detect/late-commit distance reduction attacks. The short effective symbol length also results in increased ranging resolution.

The ToA of these symbols is validated by physical layer properties and data at the logical layer. Similar to LTE, 5G uses fixed reference signals to enable phase-tracking and synchronization. An attacker can spoof these reference signals and force *out of turn* transmissions and incorrect decoding of data at the receiver resulting in false distance measurements. In contrast, V-Range does not use reference signals for the clock offset estimation, and its receiver relies on a custom algorithm for data detection. An attacker can cause distance enlargement attacks by relaying a delayed version of the challenges and responses. Moreover, an attacker can perform signal annihilation to prevent legitimate signal detection at a smart receiver. In V-Range, we implement a signal integrity checker algorithm based on inspecting the energy variance of the received symbols and show that V-Range is capable of detecting such an attempt at distance enlargement attack.

In V-Range, communicating devices perform an initialization phase and pre-share data for secure ranging. The constructed message is converted into a physical layer code using shortened OFDM symbols. These symbols

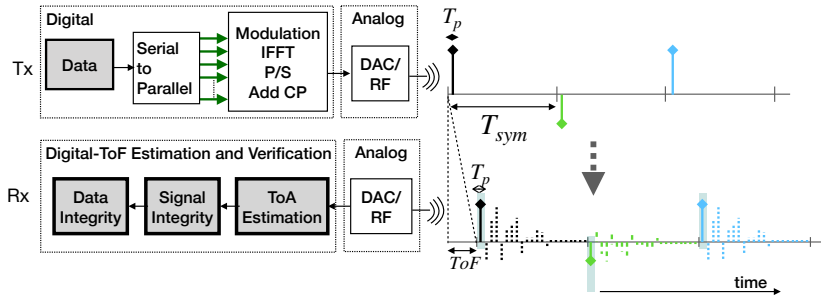


Figure 7.2: V-Range uses shortened OFDM symbols and the receiver checks the integrity of ToA estimates.

have length T_{sym} within which energy is aggregated over a much smaller part T_p of the symbol. The receiver verifies the ToA of the signal by using granular samples of length T_p, and performs the following integrity checks. The signal is considered a legitimate message for ToA estimation if the average power of these samples is more than the noise threshold (T_{Noise}) and less than threshold (T_{max}). The threshold T_{max} is used to detect the possibility of the receiver's saturation; if an attacker overloads the receiver with too much power (*e.g.,* jamming signal), then the data cannot be recovered. Each receiver can select T_{max} based on its maximum acceptable power (*i.e.,* dynamic range). The signal is used for ranging only after signal integrity (*i.e.,* power distribution) and data integrity validation.

7.2.2 System Design (Code Generation and Verification)

Generating short 5G symbols: OFDM achieves high throughput by modulating different data bits over subcarriers, resulting in the energy distribution over the symbol of length T_{sym}, as shown in Figure 7.3a. However, a secure ranging system does not require high throughput, and our design exploits the same. In contrast to transmitting different data on the subcarriers, V-Range modulates the same data on all subcarriers. This results in a specially shaped symbol with a length same as that of original OFDM but with an energy aggregated over a much smaller part T_p of the symbol, as shown in Figure 7.3b.

In OFDM, the Inverse Fast Fourier Transform (IFFT) is applied to subcarriers to generate the time-domain signal. The subcarriers' amplitude is scaled depending on the data modulated on them and then added together. If subcarriers carry different data bits, the signal's energy is distributed over $\hat{N}$ time samples and T_{sym} duration. When the subcarriers

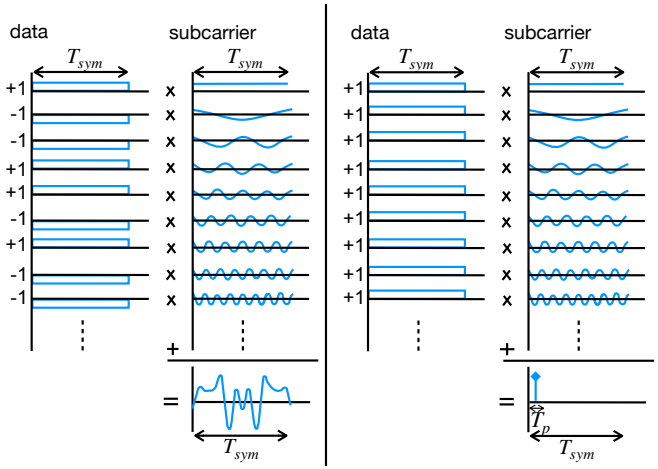


Figure 7.3: The shortened OFDM symbols are generated by modulating all subcarriers with the same data.

are modulated with the same data (*i.e.,* subcarriers have the same energy), all samples except one cancel each other. The symbol's length (T_{sym}) is unmodified, and the symbol has $\hat{N}$ samples. However, the energy is aggregated over a duration T_p where $T_p << T_{sym}$. At the receiver, the samples collected within this T_p part of the symbol are sufficient to decode the data. The remaining part of the symbol at the receiver only contains noise as no signal energy was present during transmission. Below, we formally describe these specialized OFDM symbols. Each OFDM symbol can be described as a complex-valued function $s(t)$ in the time domain. $s(t)$'s real and imaginary parts (I/Q data) represent in-phase and quadrature components. An OFDM symbol is then expressed as the aggregation of the contributions of all $\hat{N}$ subcarriers:

$$s(t) = \sum_{k=0}^{\hat{N}-1} X_k \cdot e^{j2\pi kt/T}, \quad \text{where } t \in [-T_g, T_{sym})$$

and X_k is the constellation point encoded on subcarrier $e^{j2\pi kt/T}$. In fact, this is just the IFFT on the complex data elements X_k evaluated over the length of the symbol and the guard interval T_g [115]. If all the data elements are

equal, i.e., $X_k \equiv X \in \mathbb{C}$, we simplify this formula to:

$$s(t) = X \cdot \sum_{k=0}^{\hat{N}-1} e^{j2\pi kt/T_{sym}} = X \cdot \sum_{k=0}^{\hat{N}-1} \left(e^{j2\pi t/T_{sym}}\right)^k$$

If $t = p \cdot T_{sym}$ for any integer $p \in \mathbb{Z}$, then $e^{j2\pi t/T_{sym}} = 1$ and thus $s(t) = X \cdot \hat{N}$. Since $t \in [-T_g, T_{sym})$ and $T_g < T_{sym}$, this condition is only satisfied when $p = 0$. In case $e^{j2\pi t/T_{sym}} \neq 1$, the geometric series can be rewritten as:

$$s(t) = X \cdot \frac{1 - e^{\rho\hat{N}}}{1 - e^{\rho}} = \frac{e^{-\rho\frac{\hat{N}}{2}} - e^{\rho\frac{\hat{N}}{2}}}{e^{-\rho\frac{1}{2}} - e^{\rho\frac{1}{2}}} \cdot \frac{e^{\rho\frac{\hat{N}}{2}}}{e^{\rho\frac{1}{2}}} \cdot \frac{2j}{2j}$$

$$= X \cdot \frac{\sin(\pi\hat{N}t/T_{sym})}{\sin(\pi t/T_{sym})} \cdot e^{j\pi(\hat{N}-1)t/T_{sym}} \tag{7.1}$$

where we set $\rho = j2\pi t/T_{sym}$. This is known as a (frequency-shifted) Dirichlet kernel or periodic sinc function [161].

The signal's maximum amplitude is $s(0) = X \cdot \hat{N}$, which is only attained at $t = 0$ where $s(t)$ forms a single narrow peak. Moreover, $s(t)$ has the zeroes $s(\ p \cdot \frac{T_{sym}}{\hat{N}}\ ) = 0$ for any $p \in \mathbb{Z}_{\neq 0}$. The main "lobe" of the symbol's theoretical width is, therefore, $T_p = 2\frac{T_{sym}}{\hat{N}}$, i.e., the width scales linearly with the symbol length and is inversely proportional to the number of subcarriers. Figure 7.3b) shows how $s(t)$ is composed of the different subcarriers. It is apparent that the energy is focused on a single narrow peak. Figure 7.11a in the experimental evaluation depicts over-sampled symbols $s(t)$ from an actual transmission for different subcarrier bandwidths.

The number of unique symbols with such a structure depends on X. Any digital modulation can be used to encode data in X, independent of the number of subcarriers. We explore the choice of modulation scheme in Section 7.4 to find a performant and secure configuration. We do not need high-order modulation for ranging, as these symbols are intended to be used as reference symbols for ranging. We also point out that physical channel features (*e.g.,* pilot subcarriers and the cyclic prefix required for channel estimation), normally a part of OFDM symbols, are not available in our modified symbols. These symbols' advantage is that they exhibit single carrier symbols' properties even though they are valid multi-carrier OFDM symbols. Due to single carrier properties, there is no inter-carrier interference or subcarrier phase rotation, allowing for a simple receiver design that supports secure ranging.

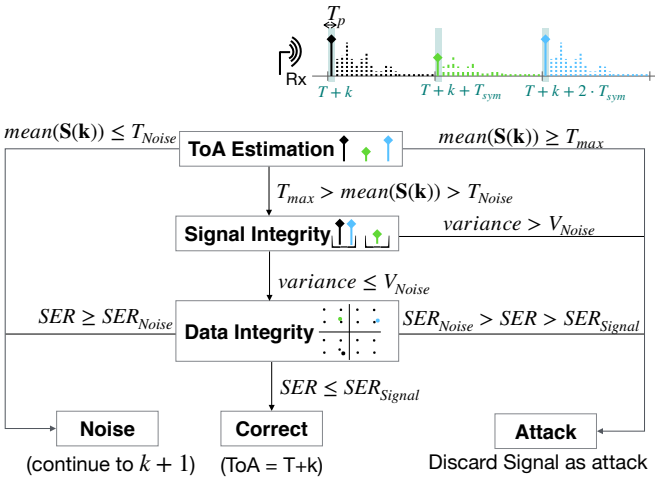


Figure 7.4: The signal received at the estimated ToA is verified using signal and data integrity checks. The mean power, variance, and symbol error threshold differentiate between noise, legitimate, and attack signals.

ToA Estimation: The estimation of a symbol's time-of-arrival is key to a precise distance measurement. Assuming that a ranging symbol is transmitted at time T, it arrives at the receiver at time $T + ToF$, where ToF depends on the signal's propagation time between the devices. Recall that unlike standard OFDM, where energy is distributed over the entire symbol duration T_{sym}, V-Range OFDM symbol's energy is concentrated over a much smaller duration. Therefore, the receiver estimates arrival time by using fine-grained samples of duration T_p. The receiver starts the search at an offset of k samples and continues until it finds the legitimate symbol (or attack traces). As the transmitter sends more than one but n consecutive ranging symbols, the receiver can use all these symbols for ToA estimation and validation. The samples that fall on to the n symbols at offset k are represented as the set $\mathbf{S(k)}$ and are collected at times $T + k + i \cdot T_{sym}$.

By using these samples, the receiver needs to differentiate between legitimate signal, adversarial signal, multi-path components, and noise. The receiver starts by checking the samples' average power. If power $< T_{Noise}$, the samples are discarded as noise and receiver continue the search at offset $k = k + 1$. If it is $> T_{max}$, then the signal is discarded as an attack, and a new ranging operation is initiated. If average power is between

thresholds, the offset k is considered as a probable leading edge, and the receiver performs integrity checks for ToA validation.

Signal Integrity Checker: The validity of the physical layer is crucial for secure distance measurement. The signal integrity is checked using the signal's statistical properties (*e.g.,* total power (UWB-ED design in Chapter 5) or variance [94]). For the QAM modulated signal, power thresholds are useful for ToA estimation, but variance-based checks are required for ToA verification. The power thresholds are not sufficient to differentiate between legitimate and attack signals, as a receiver cannot predict the channel's path loss with certainty. Variance, on the other hand, depends on the receiver's noise profile, *i.e.,* V_{Noise}, and increased variance can indicate the presence of interference or attack signal.

In the absence of an attacker, power distortion can happen due to two reasons: i) inter-symbol interference, and ii) dynamic environment/channel conditions. Inter-symbol interference is the result of the multipath components interfering with subsequent symbols. The V-Range OFDM symbols prevent inter-symbol interference as maximum delay spread is less than $T_{sym} - T_p$; the total time interval during which various multipath components with significant energy arrive at the receiver can only reach up to a few hundred *ns* [162], while the samples with the transmission energy are spaced in the order of μs. The signal distortion can also occur due to the changing channel condition in the dynamic environment; the signal reflects from nearby objects and buildings, moving vehicles, *etc.*. In V-Range, all ranging symbols are transmitted within the channel's coherence time, *i.e.,* the channel conditions remain relatively constant for the entire duration of the ranging slot. For example, two energy samples transmitted at time T and $T + T_{sym}$, will experience the same channel, *i.e.,* traveled same distance, reflected by the same objects *etc.*, and therefore should experience same power level distortions. Symbols received after the channel coherence time cannot be guaranteed to exhibit similar properties.

The signal integrity check exploits the above property to verify signal integrity. The signal transmitted with the same power, if experience the same channel conditions, should have the same received power. Although they can have residual variance up to V_{Noise} due to the receiver's noise, the receiver can check the power profile of the signal against a series of expected symbols (in our case, it will be the expected challenge/response). If data is not known at the receiver in advance, it can cluster the samples according to their power levels before checking the variance. The receiver

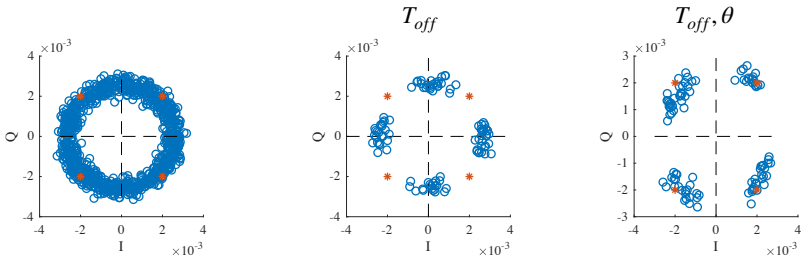


Figure 7.5: The residual frequency creates an imbalance in the in-phase and quadrature components of the signal. All samples transmitted within T_{off} duration can be demodulated by using the same value of θ.

computes the variance over the samples transmitted with the same power level, and if it exceeds V_{Noise}, the entire signal is discarded as an instance of attack. If the variance is lower than V_{Noise} for all expected power levels, the signal is passed on to the data integrity checker.

Data Integrity Checker After verifying the ranging symbols' physical-layer integrity, the V-Range receiver checks the received data's correctness by checking the symbol errors, *i.e.,* the difference between the received symbols and expected symbols. The symbol error rate SER depends on the channel conditions (*i.e.,* SNR) and hardware clock inaccuracies (*i.e.,* carrier frequency offset). Some modulation schemes withstand diverse channel conditions and higher clock inaccuracies than others. The channel conditions cannot be accurately predicted in advance, and the device can only determine the worst channel condition (*i.e.,* minimum SNR) under which a modulation scheme can operate.

As discussed in the previous chapter (see Section 6.3), secure ranging applications cannot use reference signals to correct CFO. The CFO results in in-phase and quadrature-component imbalance, which can make data recovery infeasible. The V-Range OFDM symbols modulate the same data on all subcarriers; therefore, symbols can be demodulated as single-carrier symbols without considering the rotation of each sub-carrier individually. The V-Range receiver can make use of simpler approaches to estimate frequency and phase offset. For example, the receiver can exhaustively search for these variables to recover the correct data. The exhaustive search can be avoided using optimal techniques, *e.g.,* search for the frequency offset can be avoided if the first and last symbol has a relative rotation within

a certain threshold. The frequency offset effect manifests itself in a rotation of the constellation diagram, as shown in Figure 7.5a. Although we cannot predetermine the clock inaccuracy transmitter and receiver experience at a particular time, the devices can still estimate the maximum clock inaccuracy (*i.e.,* maximum carrier frequency offset) they can experience. Therefore, if the first and last symbol of the ranging slot has a relative rotation of less than a certain ϵ, an exhaustive search for the frequency offset is not needed. Figure 7.5b shows the constellation representation of the symbols transmitted in time T_{off}. The length $T_{off} = \epsilon/(2\pi\Delta_{max})$, where Δ_{max} is maximum frequency offset between the devices and ϵ is acceptable relative rotation. As Figure 7.5c shows, the correct phase offset (θ) yields the correct symbols. The search space for the values for ϵ and θ depends on the modulation scheme [163].

The allowed symbol error rate is both a performance and a security parameter. V-Range allows symbol errors up to SER_{Signal} to perform under diverse channel conditions with hardware of different capabilities. The signal with symbol error more than SER_{Noise} is considered noise. However, the system can be considered secure only if it is infeasible for an attacker to achieve an error of less than SER_{Signal} or force a legitimate signal to have an error more than SER_{Noise} without increasing its variance.

Resource Allocation: V-Range requires consecutive sub-carriers for the short-symbol generation, and these symbols should be transmitted within the channel coherence time. The wider bandwidth and wider sub-carrier bandwidth allocation are favorable to the V-Range design. The wide bandwidth provides better security and accuracy guarantees. 3GPP is discussing to provide wider sub-carrier bandwidth, which would reduce the symbol duration T_{sym}, allowing transmission of more V-Range symbols during the same time. We only need symbol length T_{sym} slightly higher than the delay spread; the channel is underutilized when using narrow subcarrier bandwidth. Like any ToF/ToA based ranging technique (e.g., PRS), V-Range also needs to announce its presence using an upper-layer protocol, and ToF/ToA estimation from multiple stations is needed for the position estimation [112]. The repetition frequency of the V-Range messages and the choice of the distance bounding protocol (*e.g.,* one-to-one, group) depends on the use cases 5G-NR supports.

7.3 Security Analysis

The V-Range's shortened OFDM symbols are comparable to a *sequence of single-pulse bits*, since the energy of the symbol is aggregated in one sample

of duration T_p ($\approx$ few ns). The verification function is the combination of signal and data integrity checks; the signal is used for ToA if the mean power of the received signal is above T_{Noise}, its variance is less than V_{Noise} and symbol error is below SER_{Signal}. The signal is otherwise discarded as noise or an attack.

We assume that the attacker is aware of the code-generation and verification functions and the values that the receiver uses for the different decision parameters, *i.e.,* T_{Noise}, V_{Noise}, SER_{Noise}, and SER_{Signal}. However, as mentioned before, we assume that challenge and response messages are cryptographically secure, we assume that the attacker cannot predict the data transmitted using shortened OFDM symbols. The attacker has access to the samples already emitted by the legitimate transmitter and can precisely align its attack signal with the legitimate transmission. Strictly speaking, when the legitimate transmitter is transmitting the t^{th} sample, the attacker has access to all $t-1$ legitimate samples (equivalent to $\delta = 1$ according to the MTAC definition in Section 2.4), where each sample's duration is a few nanoseconds, *i.e.,* $T_p \approx 2.5\,\text{ns}$ and $T_p \approx 10\,\text{ns}$ for a system bandwidth of 400 MHz and 100 MHz respectively.

7.3.1 Distance Reduction Attack

In ToA based ranging systems, if the data is unpredictable, the attacker needs to create an illusion of an earlier arrival time by manipulating the symbol structure, *i.e.,* execute an ED/LC attack. The information leaked by the samples already transmitted by the legitimate transmitter is instrumental in such attack strategies. In the following, we show that FFT-based receivers commonly used to reconstruct the data modulated on the subcarriers of OFDM symbols do not provide secure ranging, even when used with our shortened OFDM symbols. We then analyze the security guarantees of V-Range and highlight the importance of using a combination of secure code generation and verification algorithms.

Early-detect & Late-commit: 5G uses long OFDM symbols (order of μs) to transmit data, and it is therefore vulnerable to ED/LC attacks. The attacker manipulates the receiver in measuring an earlier arrival time by producing correct data on the samples arriving earlier than the legitimate samples. To reconstruct the data transmitted on the sub-carriers (X_k), an FFT-based receiver uses all $\hat{N}$ samples, *i.e.,* $s(t)$ at $0 \leq t < \hat{N}-1$.

$$X_k = \sum_{t=0}^{\hat{N}-1} s(t) \cdot e^{-j2\pi kt/\hat{N}}, \quad \text{where } k = 0, ..., \hat{N}-1$$

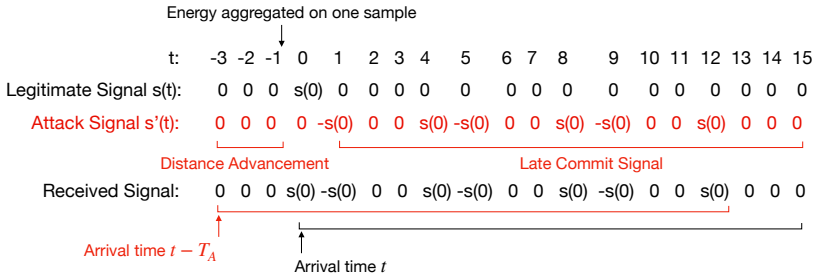


Figure 7.6: An example of the ED/LC attack on the V-Range symbol when a receiver performs FFT for data detection.

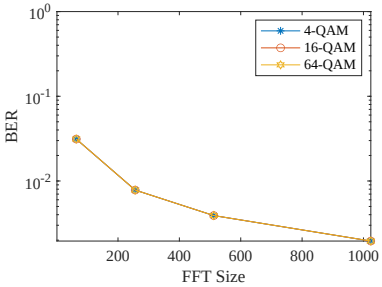


Figure 7.7: Bit error when attacker perform late commit attack on the V-Range OFDM symbol, and attack signal is procesed by FFT-based receiver.

Let us assume we use an FFT-based receiver design with the shortened OFDM symbols *i.e.,* concentrate energy within a short duration $T_p \ll T_{sym}$ by emitting only one sample with amplitude greater than zero for every symbol, as described in Section 7.2.2. In that case, the attacker will learn about the symbol structure and the data encoded in the symbol after receiving the very first sample of the symbol, i.e., $s(0)$. In order to achieve a distance reduction of α samples duration (*i.e.,* $T_A = \alpha * T_p$), the attacker can commit the next $\hat{N} - \alpha$ samples such that when the receiver uses samples $\alpha \leq t < \hat{N} - \alpha$ to perform demodulation, it results in the correct data.

Example Strategy: We show a simple strategy to generate a late commit signal as shown in Figure 7.6. An attacker can send a late commit signal to achieve advancement of $\alpha = 3$ samples, which translates to 9 m distance

reduction for the system bandwidth of 100 MHz (a lower bandwidth leads to even greater distance reduction). After observing sample $s(0)$ from the legitimate transmitter, an attacker can define late commit signal for $t = [1 \;\; \hat{N} - \alpha - 1]$ as

$$s'(t) = \begin{cases} s(0), & \text{if } t = 4, 8, 12, .. \\ -s(0), & \text{if } t = 1, 5, 9, .. \\ 0, & \text{otherwise} \end{cases}$$

The bit error depends largely on the FFT size ($\hat{N}$), as shown in Figure 7.7. This is one example strategy an attacker can implement for a late commit attack. An attacker can construct strategies targeting particular modulation schemes and FFT window sizes to further advance the signal's arrival time (*i.e.,* higher value of α).

On the other hand, the V-Range receiver treats each sample independently—the receiver is only interested in sample $s(0)$ of each symbol and does not combine the samples collected at $t > 0$ for the symbol detection. In order to advance arrival time by α sample duration, attacker needs to early commit the sample $s'(-\alpha)$ at $t = -\alpha$ before the transmission of the legitimate sample $s(0)$ at $t = 0$. There is no information leakage about $s(0)$ from samples collected at $t \leq -\alpha - 1$, the attack success depends on successful guessing. V-Range performs ToA estimation using n symbols, therefore, the attacker needs to generate the set $\mathbf{S}'(-\alpha) = \{s'_i(-\alpha) | 1 \leq i \leq n\}$ where symbol error is below $\lceil n \cdot SER_{Signal} \rceil$. The probability of generating such a sequence is given by the expression $\sum_{k=0}^{\lceil n \cdot SER_{Signal} \rceil} \binom{n}{k} (1 - 1/M)^k (1/M)^{n-k}$, where $1/M$ is the probability of correctly guessing a symbol. For example, if choosing 4-QAM as the modulation and setting $SER_{Signal} = 0.2$ and $n = 20$, the probability of attack success is 10^{-7}.

7.3.2 Distance Enlargement Attack

A secure distance measurement technique should detect the first instance/path of the legitimate signal (*i.e.,* $\mathbf{S}(0)$), even if an exact copy containing correct data is replayed with delay T_D (*i.e.,* $\mathbf{S}'(\beta)$, where $T_D = \beta * T_p$)) by an attacker. V-Range meets this requirement by ensuring that the receiver detects the legitimate signal and rejects a (replayed) attack signal. Note that the attacker cannot block the legitimate signal or prevent its detection at the receiver by generating a perfectly reciprocal signal; the duration of these samples ($\approx$ few ns) is too short to detect,

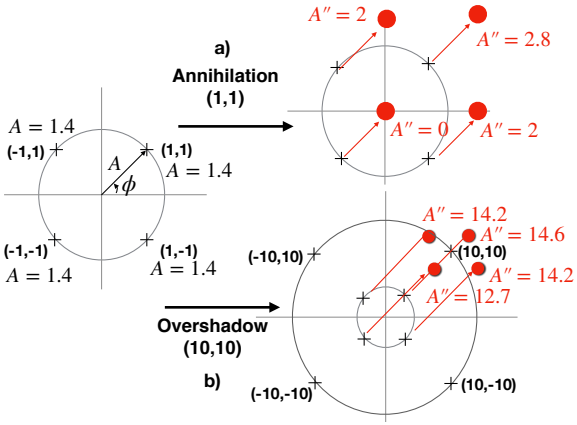


Figure 7.8: I/Q constellation in the absence and presence of the attack (annihilation and overshadowing) signal.

process, and generate a reciprocal signal. Therefore, an attacker needs to manipulate the legitimate samples by injecting noise or a structured signal in an attempt to either achieve (partial) annihilation or signal overshadowing where the legitimate signal is drowned by the attacker's transmission. If the attacker chooses to emit a structured signal, it can modify phase and amplitude as well as transmit at different carrier frequency offset(s). The attacker succeeds in distance enlargement if the manipulated signal satisfies one of the following constraints imposed by the V-Range design: (i) the mean power of the received signal is less than T_{Noise}, or (ii) it has a higher bit/symbol error rate without increasing the variance (*i.e.,* symbol error should be more than SER_{Noise} and variance less than V_{Noise}). The following analysis confirms that even a strong attacker capable of determining the expected power of the received signal cannot steer the mean and variance below the expected values (T_{Noise} and V_{Noise}).

As defined in Section 7.2.2, $s(0)$ is an I/Q sample, the modulation schemes use a set of in-phase (I) and quadrature (Q) inputs to modulate the data. For example, the 4-QAM modulation shown in Figure 7.8 have four different configuration for (I,Q) values, *i.e.,* $\mathbb{IQ}_4 = \{(I,Q)|I = \pm 1, Q = \pm 1\}$. All 4-QAM modulated symbols are transmitted with the same amplitude ($A = \sqrt{I^2 + Q^2}$) and differ only in the phase ($\phi = tan^{-1}(Q/I)$). High order modulation such as 16-QAM and 64-QAM encode data using different phase as well as different amplitude. In order to perform sample manipulation, an attacker can inject signal $s'(0)$ with in-phase I' and quadrature Q',

where amplitude is A' and phase is ϕ'. If both legitimate and attack signal arrive at the receiver at the same time, the resulting in-phase value is $I'' = I + I'$ and quadrature value is $Q'' = j(Q + Q')$, *i.e.,* both amplitude $A'' = \sqrt{(I+I')^2 + (Q+Q')^2}$ and phase $\phi'' = tan^{-1}((Q+Q')/(I+I'))$ of the received signal are affected by the signal injected by the attacker.

Reducing received power: The optimal approach to prevent detection of the received signal is signal annihilation, *i.e.,* by reducing mean power below T_{Noise}. The attacker can choose an arbitrary value for I' and Q', however, perfect cancellation is only possible when $I' = -I$ and $Q' = -Q$, *i.e.,* $A = A'$ and $\phi' = \phi + \pi$. If the I' and Q' values are chosen from the same set of legitimate transmission used for the modulation ($\mathbb{IQ}$), the probability of successful cancellation increases to $1/M$ (*i.e.,* $M = |\mathbb{IQ}|, M = 4$ for 4-QAM.). As shown by an example in Figure 7.8 for a 4-QAM signal, if the legitimate signal has amplitude $A = 1.4$, the received signal, after the cancellation attempt, has amplitude $\mathbb{A}'' = \{0, 2, 2.8\}$, with probabilities $p_1 = Pr(A'' = 0) = 0.25$, $p_2 = Pr(A'' = 2) = 0.5$ and $p_3 = Pr(A'' = 2.8) = 0.25$. As we know that each amplitude A''_k occurs with probability p_k, the probability of the occurrence of a $S''(0)$, when each amplitude A''_k occurs exactly x_k times is given by the multinomial distribution

$$Pr = \frac{n!}{x_1! \cdot \ \dots \ \cdot x_{|\mathbb{A}''|}!} p_1^{x_1} \cdot \ \dots \ \cdot p_{|\mathbb{A}''|}^{x_{|\mathbb{A}''|}} \text{ where } \sum_{k=1}^{|\mathbb{A}''|} x_k = n \tag{7.2}$$

This equation provides the probability of each configuration of amplitudes, therefore, the occurrence of different mean power, as shown in Figure 7.9a for n=20 4-QAM symbols. The probability of reducing received power below the expected power (≈ 2) is $3.3 \cdot 10^{-4}$; in all other scenarios, the presence of attack signal increases received power instead of reducing it. The probability of achieving signal cancellation for all 20 symbols is $9 \cdot 10^{-13}$, *i.e.,* when $A''_k = 0, x_k = n$ in equation 7.2

Increasing SER without increasing variance: The V-Range receiver discards any signal as noise if the SER is higher than SER_{Noise} *and* the variance of the samples transmitted with the same power is below V_{Noise}. This condition can be satisfied if the attacker steers the signal's phase while keeping the amplitude in check, *i.e.,* the receiver will recover incorrect data due to the incorrect phase estimation. As the attacker cannot manipulate the signal on the fly due to short sample duration ($\approx$ few ns), the attacker needs to inject the signal impacting both amplitude

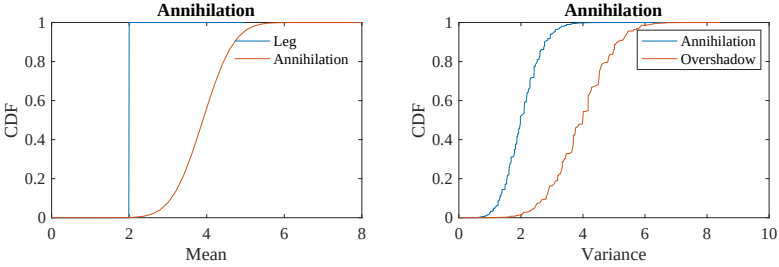


Figure 7.9: Mean and Variance of the 4-QAM modulated signal after attack.

and phase simultaneously. Therefore, an attacker cannot change the phase without manipulating the amplitude of the received signal. As shown by the example in Figure 7.8a, the amplitude of the legitimate and the attack signals is 1.4 if legitimate and attack signal is chosen from $\mathbb{IQ}_4$, the resulting amplitude $\mathbb{A}'' = \{0, 2, 2.8\}$ due to difference in the phase. Figure 7.9b shows the distribution of the variance for this $\mathbb{A}''$ for 20 symbols using equation 7.2. The probability of achieving $V_{Noise} = 0$, as required in the absence of the noise, is $9.5 \cdot 10^{-7}$. On choosing a high variance signal, where an attacker varies both amplitude and phase, the variance is only bound to increase with the higher probability. For example, when the legitimate signal is 4-QAM modulated, and an attacker injects 16-QAM modulated signal, the probability of achieving $V_{Noise} = 0$ reduces to $2.7 \cdot 10^{-12}$. The samples in the set $\mathbf{S}(0)$ are not affected by multipath components, but they experience an AWGN[1] channel. Therefore, the receiver needs to set the value of V_{Noise} based on the expected noise power spectral density and the system's bandwidth. For example, if the receiver sets $V_{Noise} = 0.5$, the probability of achieving variance below V_{Noise} is $3 \cdot 10^{-4}$, assuming that the received signal is only a combination of legitimate and attack signal selected from $\mathbb{IQ}_4$, and probability is obtained using equation 7.2.

Overshadowing legitimate signal: An attacker has to perform an overshadow attack by transmitting a high power signal with a delay $\beta = T_{sym} * k$, such that the attack signal overlaps the legitimate signal. Otherwise, the receiver will find traces of the legitimate signal and use it for the ToA estimation. The attack signal is an amplified version of the legitimate signal, *i.e.*, $s'_{i+k}(0) = \mathcal{A} \cdot s_i(0)$, where $\mathcal{A}$ is the amplification

[1] Additive White Gaussian Noise

factor. Therefore, received signal is the combination of the expected and an amplified signal, *i.e.,* $s''_{i+k}(0) = \mathcal{A} \cdot s_i(0) + s_{i+k}(0)$). This is a special case to increase the SER of the legitimate signal, by hiding it under the high power attack signal. In most cases, the receiver decodes correct data as the attack signal is simply the delayed and amplified version of the legitimate signal. However, the overlapping of the delayed high power attacker signal over the legitimate signal changes the physical layer properties; the legitimate signals behave as high variance noise interference to the attacker's signal. As shown in Figure 7.8b, the amplitude of the received signal varies due to the phase difference between legitimate and attack signal. The distribution of the variance in Figure 7.9b shows that the overshadow signal has high variance.

Carrier Frequency Offset Attack: In a traditional OFDM-based system, such as the proposed 5G numerology, an attacker can spoof the reference signals and force *out of turn* transmissions and incorrect decoding of data at the receiver resulting in false distance measurements (see Section 6.3). The V-Range design does not use reference signals for offset estimation, V-Range relies on shortened OFDM symbols, and applies integrity checks; these choices collectively make the V-Range system secure. The V-Range receiver uses short 5G symbols for CFO estimation as well as data detection; therefore, an attacker has to manipulate these symbols directly. An attacker can generate signals with different frequency and phase offset to mount an attack, such that the resulting signal, the combination of legitimate and attack signal, arrives at the receiver with different phases, and the receiver cannot recover data from this distorted signal. However, by crafting an attack signal with varying phase and frequency, the attack adds high variance to the combined signal, making it detectable at the V-Range receiver.

The V-Range design prevents all possible distance enlargement attacks as an attacker needs to generate a signal that overlaps with the legitimate signal. The combination of the legitimate and attack signal induces a detectable change in the physical layer properties of the received signal, *i.e.,* the analysis above highlights that the presence of attack signal increases the mean power and variance. This analysis shows that the V-Range detects the attempt of manipulating the first path/instance of the legitimate signal with high probability. We further examine the performance and security guarantees of the V-Range using experimental setups.

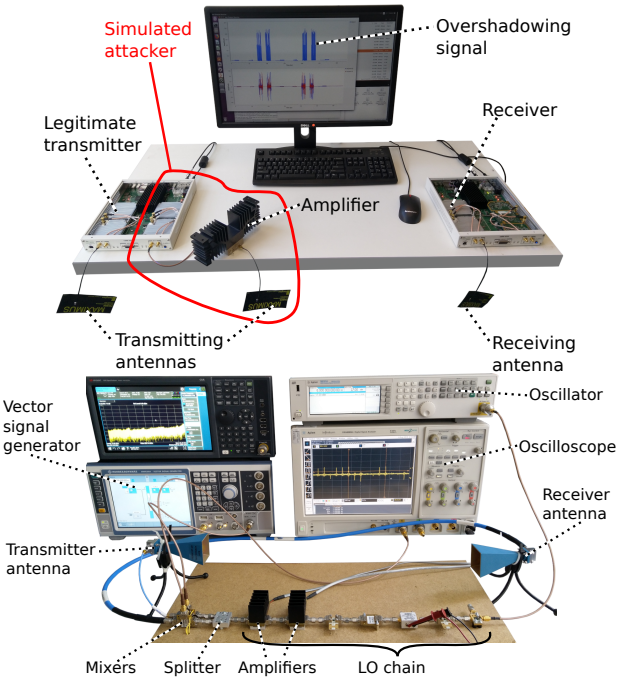


Figure 7.10: Sub-GHz and mm-wave setup.

7.4 Implementation and Evaluation

5G features a unified frame structure that supports many different physical layer configurations. The hardware designs of 5G need to be extremely flexible and are expected to use direct RF sampling techniques [164], similar to software-defined radios (SDRs) where the receive and transmit stage can be controlled at the sample level through a digital interface. Consequently, we emulate the 5G-NR physical-layer configurations with the help of SDRs for bandwidths up to 100 MHz. For higher bandwidths, we use a vector signal generator [165] since most existing SDRs currently do not support such high frequencies and bandwidths. Our results are based on two different implementations, a sub-6GHz setup and a mm-wave setup, the two frequency ranges 5G operates over. For both frequency bands, we use the maximum allowed subcarrier bandwidth (*i.e.,* shortest T_{sym}), as longer T_{sym} only increase latency.

Sub-6GHz setup: We use two USRP-X310 SDRs [166] as shown in Figure 7.10. Our setup is similar to other experimental studies on 5G [139]. Sub-carrier bandwidth is 60 kHz ($T_{sym} = 16.67\ \mu s$) and the total number of samples per symbol $\hat{N} = 2048$. With a 60 kHz sub-carrier bandwidth, the narrow peak of the resulting symbol is only $T_p \approx 10\ ns$ long. The baseband signal is generated using MATLAB and then up-converted to the center frequency $f_c = 3.4\ GHz$ by the internal mixer of the USRP before signal transmission. Both devices are using their internal clocks, which have an error of $\pm 2.5\ ppm$. The receiver operates at the same center frequency f_c and down-converts the signal without using any offset correction. The received signal is analyzed in MATLAB, which we rely on to implement the signal and data integrity checks.

mm-wave setup: We build a dedicated setup to test the performance of V-Range in the millimeter frequency bands [167, 168]. Figure 7.10 shows the transmit and receive stage that shares the same local oscillator (LO) chain for signal down- and up-conversion to $f_c = 24.5\ GHz$. The LO chain is shared to reduce the cost and size of the setup. For the mm-wave band, we again chose the maximally possible sub-carrier spacing of 480 kHz ($T_{sym} = 2.08\ \mu s$) and $\hat{N} = 256$ (*i.e.,* $T_p \approx 2ns$). The signal is transmitted and received by two identical horn antennas. We use a vector signal generator for the signal generation and an oscilloscope for the recording of the 400 MHz signal. The received signal is processed in MATLAB, similar to the Sub-6GHz setup.

In the security analysis, we will show that distance reduction and enlargement attacks are challenging to carry out against V-Range. We give advantage to the attacker by precisely aligning the attacker's signal with the legitimate signal. Therefore, when simulating an attack, we use two daughterboards of the same USRP to achieve fully synchronized transmission based on the same hardware clock (Fig. 7.10). Antennas are placed such that the travel time of the attack and legitimate signal differ at max by 1 ns. We analyze the effect of carrier frequency offset attack using simulations as we needed a controlled offset between legitimate and attack signals for analysis. We also evaluate V-Range's performance using the fading and moving propagation channel conditions [169]. A typical urban environment with rayleigh fading channel is simulated with varying doppler shifts using MATLAB's LTE toolbox [170].

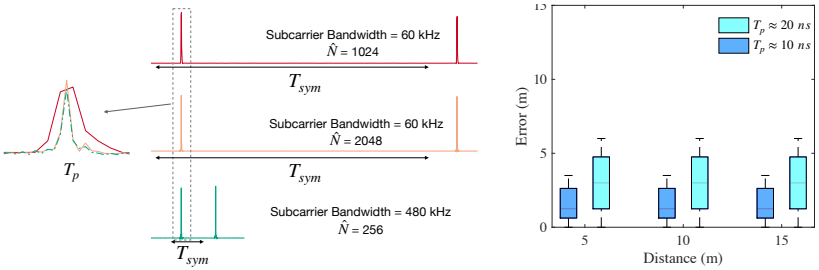


Figure 7.11: Accuracy of the distance measurement depends on the sample duration T_p

7.4.1 Parameters and Metrics

V-Range's performance depends largely on three parameters: (1) maximum expected noise variance V_{Noise}, (2) receiver signal's maximum allowable symbol error rate SER_{Signal}, and (3) maximum expected symbol error of noise SER_{Noise}. The threshold V_{Noise} is channel-independent and can be pre-estimated from the receiver's noise profile (*e.g.,* $4.5 \cdot 10^{-7}$ in our sub-6GHz setup). SER_{Noise} and SER_{Signal} are channel dependent. For example, a low SER_{Signal} increases false positives in noisy environments and high SER_{Signal} allows an attacker to make more incorrect guesses when brute-forcing a challenge and response message. Similarly, SER_{Noise} should be chosen to prevent V-Range classifying noisy environments without any legitimate ranging signal as an attack (high false positives). Furthermore, SER_{Noise} depends on the modulation scheme, *i.e.,* low SER_{Noise} for higher-order modulation (64-QAM). We evaluate V-Range's performance and security for various values of the above parameters and present our results below. Furthermore, we evaluate V-Range design's performance under different SNR conditions. We vary the transmit power and distance between devices to emulate different SNR conditions.

Ranging Duration We use 20 OFDM symbols (if not mentioned otherwise) to represent a message in our experiments to keeps chances of successful brute-force guessing low for all modulation schemes. As shown in Figure 7.12a, by correcting both frequency and phase offset, we can tolerate a longer sequence of symbols. Symbol error rate depends on channel conditions (*i.e.,* SNR) and modulation scheme. Results are shown for SNR of 8 dB; 16-QAM exhibits a higher symbol error than 4-QAM as a modulation more constellation points have more chances of error. As shown in Figure 7.12, phase offset correction is compulsory for data detection, but frequency

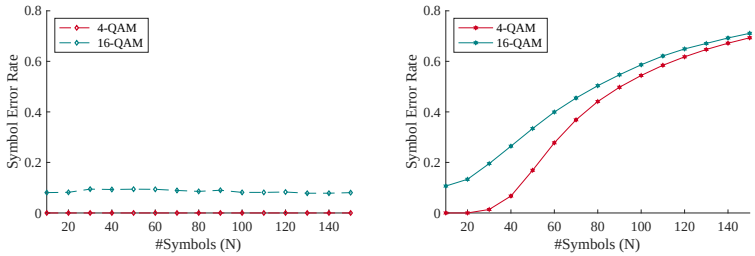


Figure 7.12: By correcting both frequency and phase offset, the device can exchange more symbols for ranging. While needing a lesser number of symbols for ranging, phase correction is sufficient.

offset correction can be made redundant when using only a few symbols and a (very) accurate clocks, such as those specified for 5G-based vehicular networks and critical systems. Offset is higher in mm-wave due to higher center frequency, the value of ϵ increases faster. However, it is compensated by shorter symbol durationT_{sym}, as shown in Figure 7.13a.

Frequency offset also leads to sampling rate mismatch between devices, which can translate into bit error as well as distance manipulation. However, the mismatch between the first and the last symbol should be more than $T_p/2$ to have any considerable effect. As shown in Figure 7.13b, the mismatch for 20 symbols is less than 10^{-2} ns for clock accuracy of .01 ppm.

Another factor that affects ranging duration is channel coherence time. A channel's coherence time is the time duration for which channel conditions remain relatively constant. Figure 7.13c show coherence time for different velocity. It is important to send V-Range symbols within coherence time to check physical layer integrity, *i.e.,* detect distance enlargement attacks using variance check. Thus, V-Range slot duration should be bounded by clock offset inaccuracies and available channel conditions (coherence time).

7.4.2 Performance Evaluation

We evaluate the performance of V-Range in terms of precision, latency, and the probability of false alarms in a benign setting.

Precision and latency: Figure 7.11 shows measurement error for sub-6GHz setup obtained under different bandwidth and distance configurations. The results show that measurement error depends only on the sample length T_p

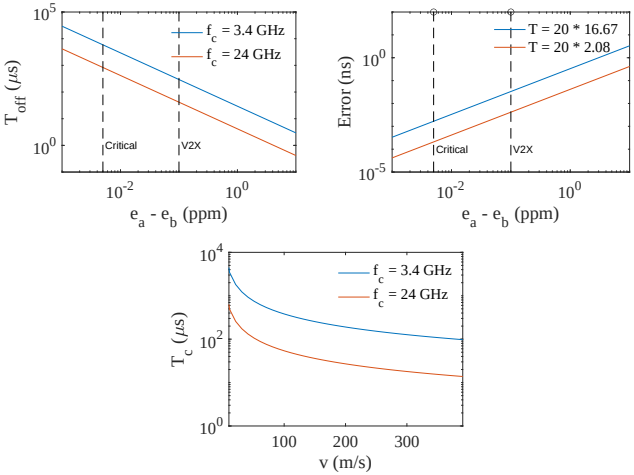


Figure 7.13: The total length of the signal recoverable at the receiver for the secure distance measurements depends on the hardware capabilities (frequency offset) and channel conditions (coherence time)

(*i.e.,* system bandwidth), independent of distances between devices. The shorter sample length T_p (*i.e.,* higher system bandwidth) achieves better precision, *e.g.,* for $T_p \approx 10$ ns, error is below 3 m. For 400 MHz bandwidth mm-wave setup, the achieved precision is 60 cm. These numbers are in line with what 3GPP expects to be attained by ranging techniques operating in 5G spectrum [145]. When performing two-way ranging, $2 \cdot n = 40$ symbols are exchanged. Thus, if symbol lengths of 16.67 μs (sub-6GHz) and 2.08 μs (mm-wave) are used, the entire ranging operation can be completed in 667 μs or 83 μs, respectively.

Effect of V_{Noise}: The signal integrity checker module monitors the received signal's power levels and raises the alarm if the variance is higher than V_{Noise}. We evaluate the probability of a legitimate signal getting discarded as an attack in Table 7.2. We observe that 4-QAM and 16-QAM signals have a low probability of triggering a false alarm, but 64-QAM signals are highly likely to be identified as an attack signal when using fewer symbols ($n = 20$). The reason is that 64-QAM sends these symbols with ten different power levels, and the sample size representing each transmits power is small - a low sample size leads to imprecise variance estimation. The performance of 64-QAM improves when using more symbols ($n = 100$).

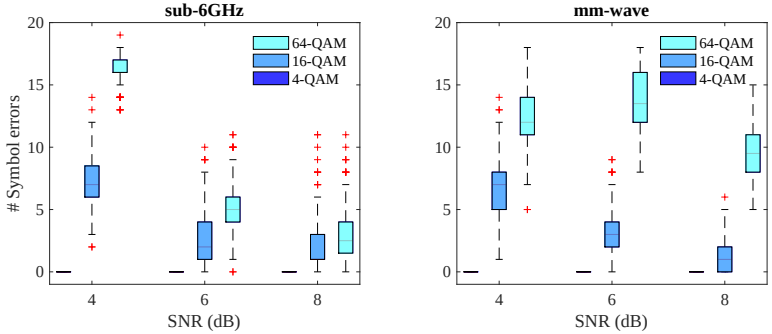


Figure 7.14: Symbol error rate of the modulation schemes depends on the channel condition (*i.e.,* SNR).

	n = 20			n = 100		
SNR [dB]	**4**	**6**	**8**	**4**	**6**	**8**
4-QAM	0	0	0	0	0	0
16-QAM	0.004	0.034	0.054	0	0	0
64-QAM	0.008	0.258	0.371	0	0.001	0.082

Table 7.2: False positives: variance estimate is imprecise when using high order modulation with a small sample size.

$(SER_{Signal}, SER_{Noise})$	Noise	Legitimate	Attack
4-QAM (0.1, 0.5)	0	1	0
16-QAM (0.3, 0.7)	0	0.913	0.086
64-QAM (0.5, 0.8)	0.0002	0.605	0.394

Table 7.3: Performance of V-Range at $SNR = 8\ dB$.

Therefore, we conclude that modulation with fewer constellations points should be used when sending fewer symbols.

Effect of SER_{Noise} and SER_{Signal}: We evaluate V-Range's performance under various SNR conditions. Figure 7.14 shows symbol errors over 100,000 challenge messages. The results are similar for sub-6GHz and mm-wave setups. 4-QAM modulation performs well even under low SNR conditions, and therefore SER_{Signal} can be set to zero. However,

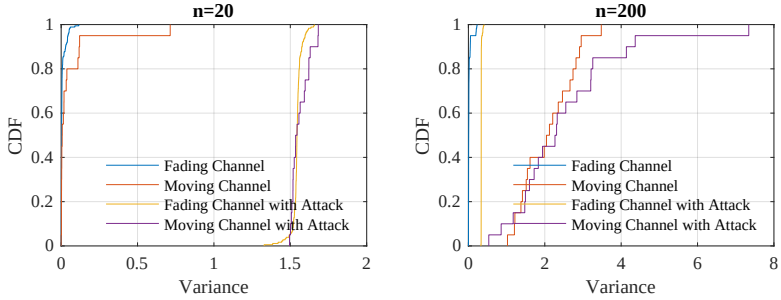


Figure 7.15: Variance on different channel conditions.

higher-order modulation schemes such as 16-QAM and 64-QAM incur symbols errors in low-SNR conditions.

For the V-Range performance presented in Table 7.3, we choose SER_{Signal} to be about 10% higher than the expected symbol error rate. Even after allowing a high value of SER_{Signal} and SER_{Noise}, 64-QAM signal has a high probability of being detected as an attack or noise. Thus, 64-QAM is not preferred when operating in low SNR conditions.

Moving Scenario: Varying channel conditions have an insignificant effect on the variance (Figure 7.15a) when all V-Range symbols are transmitted within the channel's coherence time (*i.e.,* all symbols are affected equally by multipath components). Therefore, it is possible to determine the variance threshold V_{Noise} in advance to differentiate between legitimate and attack signals. When transmission time is longer than coherence time, we see an increase in variance (Figure 7.15b). The received signal strength changes with channel condition. However, the receiver does not need to change its power thresholds T_{Noise} and T_{max} with changing scenarios. A conservative choice of T_{Noise} is always better, as it would trigger integrity checks for noise, but the receiver would not miss the legitimate signal. Similarly, T_{max} should be lower than the receiver saturation.

7.4.3 Security Evaluation

Distance Reduction Attack: V-Range is secure against ED/LC distance reduction attacks due to short effective symbol length (Section 7.3). In our setup, energy is aggregated within 10*ns* (sub-6GHz) and 2*ns* (mm-wave setup). Therefore, the maximum distance an attacker can reduce by

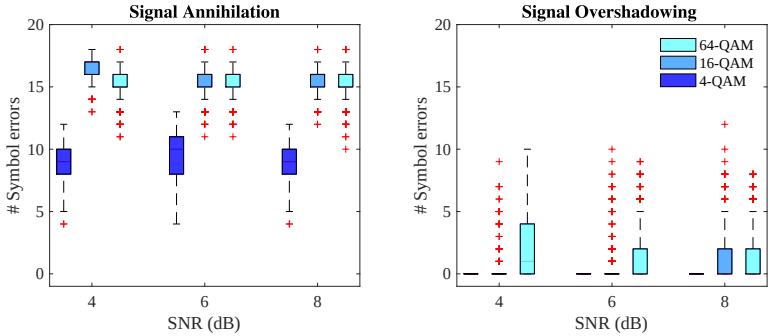


Figure 7.16: Symbol error rate in the presence of attacker.

	Annihilation			Overshadowing		
SNR [dB]	**4**	**6**	**8**	**4**	**6**	**8**
4-QAM	0.835	1	1	1	1	1
16-QAM	0.942	1	1	1	1	1
64-QAM	0.992	0.999	1	0.998	0.997	1

Table 7.4: Attack detection using integrity check.

performing ED/LC is less than 3 m and 60 cm respectively. Alternatively, the attacker can guess symbols with a guessing error below SER_{Signal}.

Distance Enlargement Attack: The distance enlargement attack's success depends on the attacker's ability to prevent the legitimate signal's detection by annihilation or overshadowing. In both attack scenarios, the attacker's signal overlaps the legitimate signal; the samples constructed at the receiver contain both the legitimate and attack signals. To validate the need for integrity checker modules, we ran 100,000 ranging operations while simulating signal annihilation and overshadow attacks.

The data integrity checker alone does not detect annihilation and overshadow attacks as the symbol error is either too high (annihilation attack) or too low (overshadowing attack)(Figure 7.16). The signal's symbol error can be $> SER_{Noise}$ in an annihilation attack. If the receiver only checks data correctness, the legitimate signal will be discarded as noise, and the attacker's signal will be used for distance estimation. In an overshadow attack, the overshadowed signal is a delayed and amplified version of the legitimate signal and resembles the legitimate signal

(symbol error $< SER_{Signal}$. Therefore, the receiver will use this delayed attack signal for distance estimation.

However, the signal's physical layer properties are changed when an attacker manipulates the legitimate signal. The signal integrity checker detects it due to the increase in the variance. The signal integrity checker results are shown in Table 7.4. We observe that annihilation and overshadow attacks are detected with high probability ($4 \cdot 10^{-5}$ false-negative rate) at SNR 8 dB. The attack detection probability of the annihilation attack is lower for the low SNR condition.

Carrier Frequency Offset Attack: We analyze carrier frequency offset attack (Section 6.3) using MATLAB's 5G toolbox on the 4-QAM modulated symbols. The designs under test are OFDM, OFDM shortened symbol with conventional receiver design where OFDM modulated reference signal is used for offset estimation, and V-Range design with the short symbol and integrity checks. We use the simulation to control the legitimate and attacker signal's frequency offset. All three configurations have no bit errors in the absence of an attacker. However, when the reference signals are overshadowed (attacker's signal power is 5dB > the legitimate signal) with different offset signals, the receiver's offset estimation is incorrect. Both OFDM and shortened OFDM symbols are vulnerable to offset attacks resulting in higher bit error (Figure 7.17). The attacker signal that arrives at the receiver with a 100 ns delay bears the correct data; therefore, the receiver uses this signal for distance estimation. The attack on OFDM and shortened OFDM symbols only differ in the sense that attack signal overlaps with the legitimate signal in OFDM as symbol duration is longer than the delay, and does not overlap in the short OFDM symbol. Therefore, OFDM symbols have incorrect data even when the offset is small.

The attack signal should fall over the legitimate signal to prevent its detection at the receiver. The legitimate and attack signals' arrival with different carrier frequency offsets inhibits the detection of the legitimate signal (higher bit error)(Figure 7.18). Due to the signal integrity checker, V-Range does not discard such a signal as noise but detects an increase in variance thereby exposing the attack.

7.5 Discussion

Compatability with LTE, WiFi, and UWB: WiFi and LTE could adopt a design similar to V-Range, but these technologies have certain limitations such as allocated system bandwidth, access control, and receiver design.

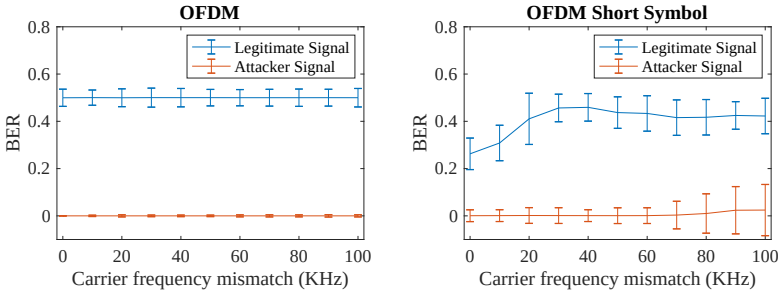


Figure 7.17: OFDM and short symbols' vulnerability to carrier frequency mismatch. The attack signal arriving after a delay β with the correct data is used for the distance measurement and the legitimate signal is discarded as noise (higher bit error).

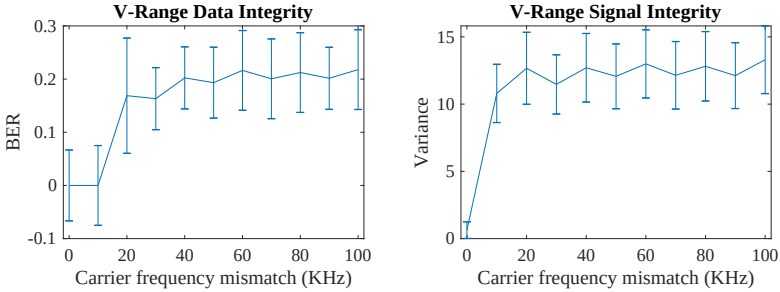


Figure 7.18: The bit/symbol error increases as legitimate and attack signals arrive with different carrier frequency offset, . However, the signal integrity checker detects the signal's distortion.

The system bandwidth in LTE limits the security guarantees, *i.e.,* longer T_s. V-Range uses the dynamic frame structure provided by 5G; LTE uses a rigid resource grid and does not allow frame aggregation and direct device-to-device communication.

Currently, there are efforts to design a secure ranging system for the WiFi 801.11az standard [171]. 802.11az will support a higher system bandwidth (up to 160 MHz) than its preceding WiFi standards and thus could support V-Range. However, WiFi's carrier-sense multiple access allocation mechanism brings a series of challenges that could result in increased false positives (noise due to packet collision) and higher latency (longer packet length, random backoff time).

UWB pulses enable short symbols and this feature heavily motivated the V-Range design. In fact, V-Range's physical layer follows the single-pulse bit sequences concept similar to the LRP in the 802.15.4z, but with extra checks and a verification function to detect distance enlargement attacks. Also, UWB and 5G serve entirely different purposes with different underlying architectures. V-Range is supposed to complement UWB ranging and support use cases and scenarios where UWB ranging is not feasible. V-Range shows how to use standard modulation schemes for ranging and performs secure ranging using coherent 5G receivers. Coherent receivers bring their own set of pros and cons, e.g., the high-order modulation mitigates guessing attacks but receivers are susceptible to carrier-frequency offset attacks if not handled explicitly.

Key Exchange and Privacy Considerations: Many 5G use cases need to maintain a shared secret for secure communication. Similar approaches can be used to generate keying material for secure ranging. The 3GPP is designing the Service Enabler Architecture Layer (SEAL) architecture to perform key exchange and secure communication in dynamic scenarios, such as vehicular networks. If a device does not have a shared secret, it can perform key exchange in the distance bounding protocol's initialization and verification phase.

Peak Power: V-Range uses shortened OFDM symbols, with energy aggregated over one sample duration. The high Peak to Average Power Ratio (PAPR) value of these symbols makes them less robust (*i.e.,* higher SER). The V-Range system is capable of handling symbol errors by using SER thresholds.

Noise, Interference and Jamming: V-Range carefully selects V_{Noise}, SER_{Signal} and SER_{Noise} to handle the receiver's noise. Any ranging system's physical layer is susceptible to interference, and is applicable for V-Range too. The presence of an interference signal leads to denial of service, as it is hard to estimate the time of arrival. We assume that the slot assignment of 5G mitigates interference. An attacker can jam the signals to launch a denial of service attack, but jamming does not lead to an incorrect distance measurement.

7.6 Conclusion

In this chapter, we proposed V-Range - the first 5G-compatible secure ranging system resilient to distance reduction and enlargement attacks.

Using shortened OFDM symbols with signal and data level integrity checks at the receiver, we designed a secure MTAC that prevents all known physical layer attacks, including the novel carrier frequency offset attack. V-Range can be readily deployed over existing 5G transceivers to achieve high precision ranging on both mm-wave and sub-6GHz frequency bands. We demonstrated that V-Range detects distance manipulation attack with a false negative rate of $\approx 10^{-5}$. Enabling such an approach in the 5G will deliver secure ranging to a wide variety of applications.

Part III

Conclusion

Chapter 8
Conclusion and Future Work

In this chapter, we summarize the work presented in this thesis and highlight the main findings and results. In addition, we remark on the lessons learned and provide directions for future work.

8.1 Summary

We began this thesis by highlighting the need for a secure relative distance measurement in the applications prevalent today. In Chapter 2, we summarized approaches used for ranging and provided an overview of the variety of distance shortening and enlargement attacks possible on these systems. We concluded that logical layer attacks can be prevented by enabling distance bounding protocols; however, they are insufficient against physical layer attacks.

In Chapter 3, we discussed the security and performance tradeoff of UWB ranging systems based on IEEE 802.15.4f/a/z standards. We showed that naively using random polarity pulses does not ensure security against distance reduction attacks. Pulses of the HRP STS are affected by multipath, and the receiver cannot differentiate if an early peak is generated in a non-adversarial (e.g., NLOS) setting or caused by a superimposed attack signal. On the other hand, LRP base mode, when used with distance bounding and distance commitment, provides secure ranging. The extended and long-range modes are still vulnerable to distance reduction by ED/LC attack. Moreover, none of these systems are designed to provide security against distance enlargement attacks. This chapter highlights the need to building secure and performant ranging systems.

In Chapter 4, we proposed UWB-PR modulation scheme that performs UWB pulse reordering and blinding on the low PRF pulses, allowing secure ranging in long-distance and NLoS conditions. The reordering prevents an attacker from learning the internal structure of the symbol to circumvent ED/LC attack. The modulation scheme, PRF, distance commitment, and receiver design are coupled uniquely, providing security against all known distance reduction attacks. UWB-PR provides quantifiable probabilistic security guarantees without making any assumptions regarding channel conditions or attacker positions.

In Chapter 5, we presented the UWB-ED modulation scheme to detect distance enlargement attacks. Similar to the UWB-PR, this approach uses

random permutation of pulses and empty slots. We showed that the receiver needs to check energy distribution and seek evidence indicating the presence of the legitimate signal even when it is distorted by the attacker. This chapter showed that signal level integrity checks are critical in detecting enlargement attacks.

In Chapter 6, we analyzed the security of the OFDM-based ranging systems, WiFi FTM and LTE/5G PRS, and exposed vulnerabilities of these ranging systems against logical and physical layer attacks. We showed that an attacker can use an indirect attack to perform distance enlargement attacks by preventing detection of the legitimate signal. We explored that the fundamental problem of using OFDM symbols for ranging is its longer symbol duration and coherent receiver design (CFO attack). We encouraged the need for building secure OFDM-based ranging systems.

Finally, in Chapter 7, we presented V-Range to enable secure positioning in 5G enabled systems. The V-Range achieves security against both distance reduction and enlargement attacks by applying sample and data level integrity checks on the shortened OFDM symbols. The effective symbols duration is reduced by modulating the same data on all subcarriers, preventing ED/LC attacks. The enlargement attack scenarios are detected by analyzing the statistical properties of the received signal.

8.2 Future Work

In this section, we provide insights for future work in the field of secure distance measurement with the end goal of designing and deploying secure and scalable positioning systems.

Security against Distance Fraud The designs we present are only secure against an external attacker (Mafia Fraud) and do not provide secure ranging if a prover is malicious. The attacker model with a malicious prover is known as Distance Fraud, and there exist approaches to thwart this attack at the logical layer [19]. However, such approaches fail when malicious prover is capable of performing physical layer attacks. Since the round-trip time includes processing time, an untrusted prover can reduce the measured distance by either sending its replies before receiving the challenges or by computing the responses faster. The prover can enlarge the measured distance by increasing processing time. Under this attacker model, we cannot detect distance enlargement, but we can design an approach to prevent distance reduction [172]. For example, when using UWB-PR, we can keep the reordering secret from the prover. The prover

would then intermingle its nonce with the verifier's challenge purely on the physical layer by adding the n_{PR} signal onto the received n_{VE} signal before transmitting the combined signal back. Because the reordering is not known to the prover, it will not be able to decode the challenge. As a consequence, the early inference of the challenge bit sequence n_{VE} can be prevented.

Scalable and secure cellular positioning: The V-Range design is the first approach that enables secure cellular positioning. Although this approach is easily deployable, it needs wide bandwidth and multiple consecutive OFDM symbols to perform ranging. The symbols used for ranging cannot be used for data transmission, therefore, reducing the overall throughput of the systems. There is a need to explore approaches that can balance the distribution of the resources between secure ranging and communication. We intend to explore two different lines of work. First, designing a physical layer that can send more symbols in a shorter time duration, *e.g.,* by reducing the spacing between the samples containing energy or by proposing even a new waveform integrated into the 5G/6G implementations. Second, the design we propose does not consider the MAC layer and distance bounding implementation. It is unclear how these protocols will be executed for use cases like V2X where connectivity to basestation may not be available, and vehicles need to perform ranging with each other. Therefore, it is important to design a framework that can enable distribution of the resources, enable scheduling, and maximize performance and security.

Location privacy: While we have achieved authenticity and integrity for ranging systems, they are not yet designed to ensure confidentiality and privacy. We need to develop policies on how the location data should be processed - who should have access to this data and when. For example, the net banking password should be changed only when the user is at a safe location. In such a case, the user's device should validate its location, possibly in a trusted execution environment, and the bank should confirm that the user is at a safe location without knowing the exact coordinates. The other entities in proximity of the user or at the communication channel should not have access to any information about the user's location [173, 174, 175]. In fact, similar privacy issues were in discussion for contact tracing apps: in this case, it is important to change the medium access control address frequently, else an adversary can track the users [176].

With the use of two-way ranging, the issues related to positioning will become more trivial. A physical layer attacker can pinpoint the device/user's location with centimeter-level precision.

8.3 Final Remarks

In this thesis, we showed that existing systems cannot be relied upon to provide secure and performant ranging in the presence of an external adversary. Specifically, we have exposed vulnerabilities of the WiFi FTM, UWB HRP and LRP, and LTE/5G PRS. We showed that using a secure logical layer and randomness at the physical layer are insufficient if a receiver cannot differentiate between noise, legitimate, and attack signals. We determined that careful selection of modulation, cryptographic operations, and detection techniques that a receiver performs to estimate and validate arrival time collectively determine if a system can be trusted. The designs we propose are the secure candidates for the Message Time of Arrival Codes and provide high security guarantees without making any assumptions regarding channel conditions. Using pulse reordering, we designed the first approach that achieves performance under longer distance and NLoS conditions without sacrificing security. We showed that such a design relaxes the principles for secure ranging. UWB-ED showed that there is a possibility of detecting enlargement attacks without using any expensive infrastructure. Lastly, we designed a secure cellular ranging system. This work is aligned with the current standardization efforts. Furthermore, we prototyped these designs and evaluated their performance, showing that they are ready for real-world deployment. Implementing them will bring about secure ranging to numerous safety- and security-critical applications. We conclude that the work of this thesis has tackled security and performance issues of the existing ranging systems and has advanced the knowledge of designing secure ranging systems.

Bibliography

[1] "Contactless Payments: The Future Of Digital Payment Technologies," https://www.csiweb.com/what-to-know/content-hub/blog/contactless-payments-the-future-of-digital-payment-technologies/, [Online; Accessed 01. July 2021].

[2] "A Mac can be unlocked by an Apple Watch," https://support.apple.com/en-gb/guide/security/secc7d85209d/web, [Online; Accessed 01. July 2021].

[3] "Near Lock," https://nearlock.me, [Online; Accessed 01. July 2021].

[4] "How to Use NFC Door Locks," https://www.getkisi.com/academy/lessons/how-to-use-nfc-door-locks, [Online; Accessed 01. July 2021].

[5] "Smart Locks: Your Entry to the Keyless World," https://www.blemobileapps.com/blog/smart-locks-entry-key-less-world/, [Online; Accessed 01. July 2021].

[6] M. Hlavác and T. Rosa, "A note on the relay attacks on e-passports: The case of czech e-passports," *IACR Cryptol. ePrint Arch.*, vol. 2007, p. 244, 2007.

[7] M.-A. Russon, "Drones to the rescue!" http://www.bbc.com/news/business-43906846, May 2018.

[8] "Six Ways Autonomous Driving is Relying on Precise Positioning," https://www.wardsauto.com/industry-voices/six-ways-autonomous-driving-relying-precise-positioning, [Online; Accessed 01. July 2021].

[9] L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, and C. Fraser, "Quantifying sars-cov-2 transmission suggests epidemic control with digital contact tracing," *Science (New York, N.Y.)*, vol. 368, no. 6491, May 2020.

[10] "COVID-19 Apps Wikipedia," https://en.wikipedia.org/wiki/COVID-19_apps/, [Online; Accessed 18. April 2021].

[11] "COVID-19 Tracking Apps," https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/, [Online; Accessed 18. April 2021].

[12] “Contactless Payments Growth,” https://www.nfcw.com/2020/05/06/366460/contactless-payments-growth-rate-doubles-in-nordic-countries/, [Online; Accessed 18. April 2021].

[13] “Contactless Payments Trend US,” https://www.forbes.com/sites/jordanmckee/2020/10/12/covid-19-is-changing-consumer-behavior-at-the-point-of-sale/?sh=7dc44adf375d, [Online; Accessed 18. April 2021].

[14] “Contactless Payments Trend,” https://about.americanexpress.com/all-news/news-details/2020/COVID-19-is-Shifting-Consumer-Purchasing-Behavior-and-Driving-U.S.-Interest-in-Contactless-Payments-According-to-2020-American-Express-Digital-Payments-Survey/default.aspx, [Online; Accessed 18. April 2021].

[15] “Relay Setup,” https://www.thesun.co.uk/motors/7804489/keyless-car-100-ebay-gadgets-relay-attacks/, [Online; Accessed 1. Feb 2021].

[16] “"mercedes ’relay’ box thieves caught on cctv in solihull.",” http://www.bbc.com/news/uk-england-birmingham-42132689, [Online; Accessed 15. June 2020].

[17] A. Francillon, B. Danev, and S. Capkun, “Relay attacks on passive keyless entry and start systems in modern cars,” in *Network and Distributed System Security Symposium (NDSS)*, 2011.

[18] “"keeping your care safe from electronic thieves.",” https://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html, [Online; Accessed November 10th 2018].

[19] S. Brands and D. Chaum, “Distance-bounding protocols,” in *EUROCRYPT*. Springer, 1994, pp. 344–359.

[20] Čapkun, Srdjan and El Defrawy, Karim and Tsudik, Gene, *Group Distance Bounding Protocols*. Springer, 2011, pp. 302–312.

[21] I. Boureanu, A. Mitrokotsa, and S. Vaudenay, “Towards Secure Distance Bounding,” Cryptology ePrint Archive, Report 2015/208, 2015, https://eprint.iacr.org/2015/208.

[22] J. Reid, J. M. G. Nieto, T. Tang, and B. Senadji, "Detecting relay attacks with timing-based protocols," in *Proceedings of the 2Nd ACM Symposium on Information, Computer and Communications Security*, ser. ASIACCS '07. ACM, 2007, pp. 204–213. [Online]. Available: http://doi.acm.org/10.1145/1229285.1229314

[23] G. P. Hancke and M. G. Kuhn, "An rfid distance bounding protocol," in *Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks*, ser. SECURECOMM '05. IEEE Computer Society, 2005, pp. 67–73. [Online]. Available: http://dx.doi.org/10.1109/SECURECOMM.2005.56

[24] A. Brelurut, D. Gerault, and P. Lafourcade, "Survey of Distance Bounding Protocols and Threats," in *Foundations and Practice of Security (FPS)*, 2015, pp. 29 – 49. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01588557

[25] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Čapkun, "Investigation of Signal and Message Manipulations on the Wireless Channel," in *Computer Security – ESORICS 2011*, V. Atluri and C. Diaz, Eds. Springer, 2011, pp. 40–59.

[26] G. Hancke, "Practical attacks on proximity identification systems," in *2006 IEEE Symposium on Security and Privacy (S P'06)*, 2006, pp. 6 pp.–333.

[27] G. P. Hancke, "Practical attacks on proximity identification systems (short paper)," in *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2006, pp. 328–333.

[28] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "Spree: A spoofing resistant gps receiver," in *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '16. ACM, 2016.

[29] "5G; study on scenarios and requirements for next generation access technologies (3gpp tr 38.913 version 14.2.0 release 14)."

[30] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What will 5g be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, June 2014.

[31] X. Cui, T. A. Gulliver, H. Song, and J. Li, “Real-time positioning based on millimeter wave device to device communications,” *IEEE Access*, vol. 4, pp. 5520–5530, 2016.

[32] E. Staudinger, M. Walter, and A. Dammann, “The 5g localization waveform ranging accuracy over time-dispersive channels – an evaluation,” 09 2016, pp. xx – xx.

[33] H. Wymeersch, G. Seco-Granados, G. Destino, D. Dardari, and F. Tufvesson, “5G mmwave positioning for vehicular networks,” *IEEE Wireless Communications*, vol. 24, no. 6, pp. 80–86, Dec 2017.

[34] “USRP B210,” https://www.ettus.com/all-products/usrp-b200mini-i-2/, [Online; Accessed 10. November 2020].

[35] P. Bahl and V. N. Padmanabhan, “RADAR: an in-building RF-based user location and tracking system,” in *IEEE INFOCOM*, vol. 2, 2000, pp. 775–784.

[36] D. Vasisht, S. Kumar, and D. Katabi, “Decimeter-level localization with a single wifi access point.” in *NSDI*, vol. 16, 2016, pp. 165–178.

[37] “3db Access AG - 3DB6830 (“proximity based access control"),” https://www.3db-access.com/Product.3.html, [Online; Accessed 23. October 2017].

[38] “DecaWave “dw1000 product description and applications",” https://www.decawave.com/products/dw1000, [Online; Accessed 23. October 2017].

[39] “LTE Positioning Protocol (LPP),” https://www.etsi.org/deliver/etsi_ts/136300_136399/136355/13.00.00_60, [Online; Accessed 12. January 2021].

[40] I. Guvenc, Z. Sahinoglu, P. Orlik, and H. Arslan, “Searchback algorithms for toa estimation in non-coherent low-rate ir-uwb systems,” *Wireless Personal Communications*, vol. 48, pp. 585–603, 03 2009.

[41] D. Dardari, A. Conti, U. Ferner, A. Giorgetti, and M. Win, “Ranging with ultrawide bandwidth signals in multipath environments,” *Proceedings of the IEEE*, vol. 97, pp. 404 – 426, 03 2009.

[42] I. Sharp, K. Yu, and Y. J. Guo, "Peak and leading edge detection for time-of-arrival estimation in band-limited positioning systems," *IET communications*, vol. 3, no. 10, pp. 1616–1627, 2009.

[43] "Volkswagen UWB PKES," https://www.volkswagen-newsroom.com/en/stories/realtime-safety-with-uwb-5438, [Online; Accessed 20. March 2021].

[44] "LRP deployment in automotive." https://www.3db-access.com/article/18, [Online; Accessed 25. March 2021].

[45] "System reference document (srdoc); short range devices (srd) using ultra wide band (uwb); technical characteristics and spectrum requirements for uwb based vehicular access systems for operation in the 3,4 ghz to 4,8 ghz and 6 ghz to 8,5 ghz frequency ranges," *IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)*, 2016.

[46] A. Ranganathan and S. Capkun, "Are we really close? verifying proximity in wireless systems," *IEEE Security Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[47] "Radio attack lets hackers steal cars with just $20 worth of gear." https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/, [Online; Accessed November 10th 2018].

[48] ""secukey"," www.secukey.org, [Online; Accessed December 20th 2020].

[49] J. Wang, K. Lounis, and M. Zulkernine, "Cskes: A context-based secure keyless entry system," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1, 2019, pp. 817–822.

[50] W. Choi, M. Seo, and D. Lee, "Sound-proximity: 2-factor authentication against relay attack on passive keyless entry and start system," *Journal of Advanced Transportation*, vol. 2018, pp. 1–13, 01 2018.

[51] T. E. Humphreys, "Assessing the spoofing threat: Development of a portable gps civilian spoofer," in *Institute of Navigation GNSS (ION GNSS)*, 2008.

[52] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your GPS are belong to us: Towards stealthy manipulation of road navigation systems," in *27th USENIX Security Symposium (USENIX Security 18)*. Baltimore, MD: USENIX Association, Aug. 2018, pp. 1527–1544. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/zeng

[53] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Capkun, "On the requirements for successful gps spoofing attacks," in *Proceedings of the 18th ACM conference on Computer and communications security*. ACM, 2011, pp. 75–86.

[54] P. Papadimitratos and A. Jovanovic, "Gnss-based positioning: Attacks and countermeasures," in *MILCOM 2008 - 2008 IEEE Military Communications Conference*, 2008, pp. 1–7.

[55] H. Sathaye, G. LaMountain, P. Closas, and A. Ranganathan, "Semperfi: A spoofer eliminating GPS receiver for uavs," *CoRR*, vol. abs/2105.01860, 2021. [Online]. Available: https://arxiv.org/abs/2105.01860

[56] S. Narain, A. Ranganathan, and G. Noubir, "Security of gps/ins based on-road location tracking systems," in *2019 IEEE Symposium on Security and Privacy (SP)*, 2019, pp. 587–601.

[57] L. Flueratoru, S. Wehrli, M. Magno, and D. Niculescu, "On the energy consumption and ranging accuracy of ultra-wideband physical interfaces," in *GLOBECOM 2020 - 2020 IEEE Global Communications Conference*, 2020, pp. 1–7.

[58] N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "Uwb rapid-bit-exchange system for distance bounding," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, ser. WiSec '15. ACM, 2015, pp. 2:1–2:12. [Online]. Available: http://doi.acm.org/10.1145/2766498.2766504

[59] M. Poturalski, Mand Flury, P. Papadimitratos, J. Hubaux, and J. Le Boudec, "The cicada attack: degradation and denial of service in ir ranging," in *Ultra-Wideband (ICUWB), 2010 IEEE International Conference on*, vol. 2. IEEE, 2010, pp. 1–4.

[60] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Distance bounding with ieee 802.15.4a: Attacks and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 10, no. 4, pp. 1334–1344, 2011.

[61] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. Le Boudec, "Effectiveness of distance-decreasing attacks against impulse radio ranging," in *Proceedings of the Third ACM Conference on Wireless Network Security*, ser. WiSec '10. ACM, 2010, pp. 117–128.

[62] ""getting started with ibeacon"," https://developer.apple.com/ibeacon/Getting-Started-with-iBeacon.pdf, [Online; Accessed 05 January 2021].

[63] "COVID-19 Apps Design," https://news.mit.edu/2020/bluetooth-covid-19-contact-tracing-0409, [Online; Accessed 18. April 2021].

[64] "Atmel phase difference measurement," http://www.atmel.com/Images/Atmel-8443-RTB-Evaluation-Application-Software-Users-Guide_Application-Note_AVR2152.pdf, [Online; Accessed 23. October 2017].

[65] R. Miesen, A. Parr, J. Schleu, and M. Vossiek, "360 degree carrier phase measurement for uhf rfid local positioning," *2013 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*, pp. 1–6, 2013.

[66] I. S. Association *et al.*, "Ieee std 802.11-2016, ieee standard for local and metropolitan area networks—part 11: Wireless lan medium access control (mac) and physical layer (phy) specifications, 2016."

[67] Zebra Technologies, ""sapphire dart ultra wideband (uwb) real time locating system 2010."," https://www.zebra.com/us/en/solutions/location-solutions/enabling-technologies/dart-uwb.html, [Online; Accessed 22. October 2018].

[68] "Apple U1 UWBChip, howpublished="https://support.apple.com/guide/security/ultra-wideband-security-sec1e6108efd/web"," [Online; Accessed 24. March 2021].

[69] "SamsungUWB," https://news.samsung.com/global/samsung-expects-uwb-to-be-one-of-the-next-big-wireless-technologies/, [Online; Accessed 24. March 2021].

[70] L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *Security and Privacy in the Age of Ubiquitous Computing*, R. Sasaki, S. Qing, E. Okamoto, and H. Yoshiura, Eds. Boston, MA: Springer US, 2005, pp. 223–238.

[71] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun, "Distance hijacking attacks on distance bounding protocols," in *2012 IEEE Symposium on Security and Privacy*, 2012, pp. 113–127.

[72] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. 29, no. 2, pp. 198–208, 1983.

[73] M. Cagalj, S. Čapkun, R. Rengaswamy, I. Tsigkogiannis, M. Srivastava, and J. Hubaux, "Integrity (I) codes: message integrity protection and authentication over insecure channels," in *IEEE Symposium on Security and Privacy (S&P)*, 2006, pp. 15 pp.–294.

[74] S. Gollakota, N. Ahmed, N. Zeldovich, and D. Katabi, "Secure in-band wireless pairing," in *USENIX Security Symposium*, 2011.

[75] G. Avoine, M. A. Bingöl, I. Boureanu, S. Čapkun, G. Hancke, S. Kardaş, C. H. Kim, C. Lauradoux, B. Martin, J. Munilla *et al.*, "Security of distance-bounding: A survey," *ACM Computing Surveys (CSUR)*, vol. 51, no. 5, pp. 1–33, 2018.

[76] K. Rasmussen and S. Capkun, "Realization of rf distance bounding," 09 2010, pp. 389–402.

[77] S. Drimer and S. J. Murdoch, "Keep your enemies close: Distance bounding against smartcard relay attacks," in *16th USENIX Security Symposium (USENIX Security 07)*. Boston, MA: USENIX Association, Aug. 2007. [Online]. Available: https://www.usenix.org/conference/16th-usenix-security-symposium/keep-your-enemies-close-distance-bounding-against

[78] D. Singelee and B. Preneel, "Location verification using secure distance bounding protocols," in *IEEE International Conference on Mobile Adhoc and Sensor Systems Conference, 2005.*, 2005, pp. 7 pp.–840.

[79] Y.-c. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Networks*, vol. 11, 10 2002.

[80] S. Čapkun, M. Čagalj, G. Karame, and N. O. Tippenhauer, "Integrity regions: Authentication through presence in wireless networks," *IEEE Transactions on Mobile Computing*, vol. 9, no. 11, pp. 1608–1621, 2010.

[81] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: Association for Computing Machinery, 2009, p. 410–419. [Online]. Available: https://doi.org/10.1145/1653662.1653712

[82] H. T. T. Truong, X. Gao, B. Shrestha, N. Saxena, N. Asokan, and P. Nurmi, "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)*, 2014, pp. 163–171.

[83] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis, "Practical relay attack on contactless transactions by using nfc mobile phones," 2012.

[84] H. Ólafsdóttir, A. Ranganathan, and S. Čapkun, "On the security of carrier phase-based ranging," in *International Conference on Cryptographic Hardware and Embedded Systems*. Springer, 2017, pp. 490–509.

[85] S. Sedighpour, S. Čapkun, S. Ganeriwal, and M. Srivastava, "Distance enlargement and reduction attacks on ultrasound ranging," in *Proceedings of the 3rd International Conference on Embedded Networked Sensor Systems*, ser. SenSys '05. New York, NY, USA: Association for Computing Machinery, 2005, p. 312. [Online]. Available: https://doi.org/10.1145/1098918.1098977

[86] G. Avoine, I. Boureanu, D. Gérault, G. P. Hancke, P. Lafourcade, and C. Onete, *From Relay Attacks to Distance-Bounding Protocols*. Cham: Springer International Publishing, 2021, pp. 113–130. [Online]. Available: https://doi.org/10.1007/978-3-030-10591-4_7

[87] L. Taponecco, P. Perazzo, A. A. D'Amico, and G. Dini, "On the Feasibility of Overshadow Enlargement Attack on IEEE 802.15.4a Distance Bounding," *IEEE Communications Letters*, vol. 18, no. 2, pp. 257–260, 2014.

[88] J. S. Warner and R. G. Johnston, "Gps spoofing countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[89] A. Ranganathan, B. Danev, A. Francillon, and S. Capkun, "Physical-layer attacks on chirp-based ranging systems," in *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. ACM, 2012, pp. 15–26.

[90] "Cyclic Prefix Replay Attack," https://mentor.ieee.org/802.11/dcn/17/11-17-1122-00-00az-cp-replay-threat-model-for-11az.pptx, [Online; Accessed 24. September 2019].

[91] J. Clulow, G. P. Hancke, M. G. Kuhn, and T. Moore, "So near and yet so far: Distance-bounding attacks in wireless networks," in *Proceedings of the Third European Conference on Security and Privacy in Ad-Hoc and Sensor Networks*, ser. ESAS'06. Springer, 2006, pp. 83–97. [Online]. Available: http://dx.doi.org/10.1007/11964254_9

[92] N. O. Tippenhauer, K. B. Rasmussen, and S. Čapkun, "Physical-layer Integrity for Wireless Messages," *Computer Networks*, vol. 109, no. P1, pp. 31–38, 2016.

[93] Humatics, "Time Domain's PulsON ("p440")," http://www.timedomain.com/products/pulson-440/, [Online; Accessed 23. October 2017].

[94] P. Leu, M. Singh, M. Roeschlin, K. G. Paterson, and S. Čapkun, "Message time of arrival codes: A fundamental primitive for secure distance measurement," in *2020 IEEE Symposium on Security and Privacy (SP)*, 2020, pp. 500–516.

[95] "UWB Social Distancing," https://www.uwb-social-distancing.com/, [Online; Accessed 22. March 2021].

[96] "UWB Social Distancing Meeblue," https://www.meeblue.com/blogs/UWB_For_Social_Alert/, [online; Accessed 20. March 2021].

[97] "Ieee standard for information technology– local and metropolitan area networks– specific requirements– part 15.4: Wireless medium access control (mac) and physical layer (phy) specifications for low-rate wireless personal area networks (wpans): Amendment 1: Add alternate phys," *IEEE Std 802.15.4a-2007 (Amendment to IEEE Std 802.15.4-2006)*, pp. 1–210, 2007.

[98] "Ieee standard for local and metropolitan area networks– part 15.4: Low-rate wireless personal area networks (lr-wpans) amendment 2: Active radio frequency identification (rfid) system physical layer (phy)," *IEEE Std 802.15.4f-2012 (Amendment to IEEE Std 802.15.4-2011)*, pp. 1–72, 2012.

[99] "802.15.4z - standard for low-rate wireless networks amendment: Enhanced high rate pulse (hrp) and low rate pulse (lrp) ultra wide-band (uwb) physical layers (phys) and associated ranging techniques," https://standards.ieee.org/develop/project/802.15.4z.html, [Online; Accessed 7. August 2018].

[100] "Microchip ATA8532," https://www.microchip.com/wwwproducts/en/ATA8352, [Online; Accessed 25. March 2021].

[101] "NXP Trimension," https://www.nxp.com/docs/en/fact-sheet/UWB-IOT-FS.pdf, [Online; Accessed 25. March 2021].

[102] "Introduction to Impulse Radio UWB Seamless Access Systems," https://www.firaconsortium.org/sites/default/files/2020-04/fira-introduction-impulse-radio-uwb-wp-en.pdf, [Online; Accessed 05. July 2021].

[103] M. Stocker, B. Großwindhager, C. A. Boano, and K. Römer, "Towards secure and scalable uwb-based positioning systems," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2020, pp. 247–255.

[104] K. Mikhaylov, J. Petäjäjärvi, M. Hämäläinen, A. Tikanmäki, and R. Kohno, "Impact of ieee 802.15.4 communication settings on performance in asynchronous two way uwb ranging," *International Journal of Wireless Information Networks*, vol. 24, no. 2, pp. 124–139, 2 2017.

[105] M. Singh, M. Roeschlin, E. Zalzala, P. Leu, and S. Čapkun, "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*, ser. WiSec '21. New York, NY, USA: Association for Computing Machinery, 2021, p. 227–237. [Online]. Available: https://doi.org/10.1145/3448300.3467831

[106] A. F. Molisch, K. Balakrishnan, C.-C. Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak, "Ieee 802.15. 4a channel model-final report," *IEEE P802*, vol. 15, no. 04, p. 0662, 2004.

[107] A. Compagno, M. Conti, A. A. D'Amico, G. Dini, P. Perazzo, and L. Taponecco, "Modeling Enlargement Attacks Against UWB Distance Bounding Protocols," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1565–1577, 2016.

[108] R. J. Fontana and E. A. Richley, "Observations on low data rate, short pulse uwb systems," in *Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on*. IEEE, 2007, pp. 334–338.

[109] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in *INFOCOM 2003*, vol. 3. IEEE, 2003, pp. 1976–1986.

[110] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on Wireless security*. ACM, 2003, pp. 1–10.

[111] S. Capkun and J.-P. Hubaux, "Secure positioning in wireless networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 221–232, 2006.

[112] S. Čapkun and J. Hubaux, "Secure positioning of wireless devices with application to sensor networks," in *IEEE Computer and Communications Societies.*, vol. 3, 2005, pp. 1917–1928.

[113] K. Witrisal, G. Leus, G. J. M. Janssen, M. Pausini, F. Troesch, T. Zasowski, and J. Romme, "Noncoherent ultra-wideband systems," *IEEE Signal Processing Magazine*, vol. 26, no. 4, pp. 48–66, 2009.

[114] A. F. Molisch, K. Balakrishnan, C. chin Chong, S. Emami, A. Fort, J. Karedal, J. Kunisch, H. Schantz, U. Schuster, and K. Siwiak, "IEEE 802.15.4a channel model - final report," in *Converging: Technology, work and learning. Australian Government Printing Service*. [Online; Accessed 4. November 2018], 2004.

[115] A. F. Molisch, *Wireless communications*. John Wiley & Sons, 2012, vol. 34.

[116] A. Molisch, "Ultrawideband propagation channels-theory, measurement, and modeling," *IEEE Transactions on Vehicular Technology*, vol. 54, no. 5, pp. 1528–1545, 2005.

[117] A. Muqaibel, A. Safaai-Jazi, A. Bayram, and S. M. Riad, "Ultra wideband material characterization for indoor propagation," in *IEEE Antennas and Propagation Society International Symposium*, vol. 4, 2003, pp. 623–626.

[118] A. F. Molisch, D. Cassioli, C. Chong, S. Emami, A. Fort, B. Kannan, J. Karedal, J. Kunisch, H. G. Schantz, K. Siwiak, and M. Z. Win, "A Comprehensive Standardized Model for Ultrawideband Propagation Channels," *IEEE Transactions on Antennas and Propagation*, vol. 54, no. 11, pp. 3151–3166, 2006.

[119] "LTE in a Nutshell," https://home.zhaw.ch/kunr/NTM1/literatur/LTE%20in%20a%20Nutshell%20-%20Physical%20Layer.pdf, [Online; Accessed 12. January 2021].

[120] B. M. Lee, M. Patil, P. Hunt, and I. Khan, "An easy network onboarding scheme for internet of things networks," *IEEE Access*, vol. 7, pp. 8763–8772, 2018.

[121] W.-F. Alliance, "Wi-fi aware | wi-fi alliance," https://www.wi-fi.org/discover-wi-fi/wi-fi-aware, 2020 (Accessed 3 December 2020).

[122] M. Ibrahim, A. Rostami, B. Yu, H. Liu, M. Jawahar, V. Nguyen, M. Gruteser, F. Bai, and R. Howard, "Wi-go: accurate and scalable vehicle positioning using wifi fine timing measurement," in *Proceedings of the 18th International Conference on Mobile Systems, Applications, and Services*, 2020, pp. 312–324.

[123] IEEE, "Ieee p802.11 - next generation positioning study group," http://www.ieee802.org/11/Reports/tgaz_update.htm, 2020 (Accessed 29 March 2020).

[124] N. Maziar, W. Yue, T. Milos, W. Shangbin, Q. Yinan, and A.-I. Mohammed, "Overview of 5g modulation and waveforms candidates," *Journal of Communications and Information Networks*, vol. 1, no. 1, pp. 44–60, Jun 2016.

[125] L. J. Gutierrez, Q. Wang, V. Erceg, and H. Ramakrishnan, "Wireless communication fine timing measurement phy parameter control and negotiation," Mar. 7 2017, uS Patent 9,591,493.

[126] Android, "Wi-fi location: ranging with rtt | android developers," https://developer.android.com/guide/topics/connectivity/wifi-rtt, 2020 (Accessed 18 June 2020).

[127] W.-F. Alliance, "Product finder | wi-fi alliance," https://www.wi-fi.org/product-finder, 2020 (Accessed 2 April 2020).

[128] A. Gaber and A. Omar, "A study of tdoa estimation using matrix pencil algorithms and ieee 802.11ac," in *2012 Ubiquitous Positioning, Indoor Navigation, and Location Based Service (UPINLBS)*, 2012, pp. 1–8.

[129] S. M. Sridhar and C. H. Aldana, "Secure fine timing measurement protocol," Aug. 27 2019, uS Patent 10,397,779.

[130] C. H. Aldana, A. Raissinia, S. Vamaraju, and K. Anand, "Secure fine timing measurement exchange," Aug. 28 2018, uS Patent 10,064,057.

[131] M. Ibrahim, H. Liu, M. Jawahar, V. Nguyen, M. Gruteser, R. Howard, B. Yu, and F. Bai, "Verification: Accuracy evaluation of wifi fine time measurements on an open platform," in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*. ACM, 2018, pp. 417–427.

[132] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. Association for Computing Machinery, 2008, pp. 128–139.

[133] "WLAN Channel Models," https://www.mathworks.com/help/wlan/gs/wlan-channel-models.html, [Online; Accessed 21. June 2020].

[134] S. Dwivedi, R. Shreevastav, F. Munier, J. Nygren, I. Siomina, Y. Lyazidi, D. Shrestha, G. Lindmark, P. Ernström, E. Stare, S. M. Razavi, S. Muruganathan, G. Masini, Åke Busin, and F. Gunnarsson, "Positioning in 5g networks," 2021.

[135] R. Ferre, G. Seco-Granados, and E. S. Lohan, "Positioning reference signal design for positioning via 5g," 10 2019.

[136] J. Peral-Rosado, J. A. López-Salcedo, G. Seco-Granados, F. Zanier, and C. Massimo, "Evaluation of the lte positioning capabilities under typical multipath channels," 09 2012, pp. 139–146.

[137] Qualcomm, "Snapdragon 800 Processor," https://www.qualcomm.com/products/snapdragon-processors-800, [Online; Accessed 30. October 2020].

[138] "srsLTE," https://github.com/srsLTE/srsLTE, [Online; Accessed 12. December 2020].

[139] "Open Air Interface," https://www.openairinterface.org, [Online; Accessed 16. October 2019].

[140] H. Yang, S. Bae, M. Son, H. Kim, S. M. Kim, and Y. Kim, "Hiding in plain signal: Physical signal overshadowing attack on LTE," in *28th USENIX Security Symposium (USENIX Security 19)*. Santa Clara, CA: USENIX Association, Aug. 2019, pp. 55–72. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/yang-hojoon

[141] "MATLAB PRS," https://www.mathworks.com/help/lte/ug/time-difference-of-arrival-positioning-using-prs.html, [Online; Accessed 12. December 2020].

[142] A. A. Nasir, S. Durrani, H. Mehrpouyan, S. D. Blostein, and R. A. Kennedy, "Timing and carrier synchronization in wireless communication systems: A survey and classification of research in the last five years," *CoRR*, vol. abs/1507.02032, 2015. [Online]. Available: http://arxiv.org/abs/1507.02032

[143] Y. Qi, M. Hunukumbure, H. Nam, H. Yoo, and S. Amuru, "On the phase tracking reference signal (PT-RS) design for 5g new radio (NR)," *CoRR*, vol. abs/1807.07336, 2018. [Online]. Available: http://arxiv.org/abs/1807.07336

[144] X. Lin, J. Li, R. Baldemair, T. Cheng, S. Parkvall, D. Larsson, H. Koorapaty, M. Frenne, S. Falahati, A. Grövlen, and K. Werner, "5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology," 2018.

[145] "5G - GPP 38.855 ;Technical Specification Group Radio Access Network; Study on NR positioning support," https://www.3gpp.

org/ftp/Specs/archive/38_series/38.855/, [Online; Accessed 17. June 2020].

[146] "5G for Positioning," https://www.pointr.tech/blog/5g-indoor-positioning, [Online; Accessed 05. June 2021].

[147] "5G will open new possibilities in positioning," https://www.bell-labs.com/institute/blog/5g-will-open-new-possibilities-positioning/#gref, [Online; Accessed 05. June 2021].

[148] G. Destino, J. Saloranta, G. Seco-Granados, and H. Wymeersch, "Performance analysis of hybrid 5g-gnss localization," in *2018 52nd Asilomar Conference on Signals, Systems, and Computers*, 2018, pp. 8–12.

[149] R. Crapart, R. Maymo-Camps, B. Vautherin, and J. Saloranta, "5G Positioning And Hybridization With GNSS Observations," in *ITSNT 2018, International Technical Symposium on Navigation and Timing*, Toulouse, France, Oct. 2018. [Online]. Available: https://hal-enac.archives-ouvertes.fr/hal-01942264

[150] "Proof of Concept of Hybrid 5G-NR/GNSS Positioning with AD-HOC Overlay," https://navisp.esa.int/opportunity/details/72/show, [Online; Accessed 05. July 2021].

[151] Y. Cao, C. Xiao, B. Cyr, Y. Zhou, W. Park, S. Rampazzi, Q. A. Chen, K. Fu, and Z. M. Mao, "Adversarial sensor attack on lidar-based perception in autonomous driving," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '19. New York, NY, USA: Association for Computing Machinery, 2019, pp. 2267–2281. [Online]. Available: https://doi.org/10.1145/3319535.3339815

[152] "Autonomous vehicles can be fooled to 'see' nonexistent obstacles," https://gcn.com/articles/2020/03/06/lidar-spoofs-autonomous-vehicle-hack.aspx, [Online; Accessed 05. June 2021].

[153] J. Sun, Y. Cao, Q. A. Chen, and Z. M. Mao, "Towards robust lidar-based perception in autonomous driving: General black-box adversarial sensor attack and countermeasures," 2020.

[154] "5G Americas Whitepaper Cellular V2X Communications towards 5G," https://www.5gamericas.org/wp-content/uploads/2019/07/

2018_5G_Americas_White_Paper_Cellular_V2X_Communications_Towards_5G__Final_for_Distribution.pdf, [Online; Accessed 16. June 2020].

[155] "Hybrid 5G and GPS," https://www.esa.int/Applications/Navigation/ESA_leads_drive_into_our_5G_positioning_future, [Online; Accessed 16. June 2020].

[156] A. Ghosal and M. Conti, "Security issues and challenges in v2x: A survey," 03 2019.

[157] R. Raulefs, A. Dammann, T. Jost, M. Walter, and S. Zhang, "The 5g localization waveform," 01 2016.

[158] Ericsson, "5G New Radio: Designing for the future," https://www.ericsson.com/assets/local/publications/ericsson-technology-review/docs/2017/designing-for-the-future---the-5g-nr-physical-layer.pdf, [Online; Accessed 16. June 2020].

[159] K. Witrisal, P. Meissner, E. Leitinger, Y. Shen, C. Gustafson, F. Tufvesson, K. Haneda, D. Dardari, A. F. Molisch, A. Conti, and M. Z. Win, "High-accuracy localization for assisted living: 5g systems will turn multipath channels from foe to friend," *IEEE Signal Processing Magazine*, vol. 33, no. 2, pp. 59–70, March 2016.

[160] A. Kakkavas, M. H. C. García, R. A. Stirling-Gallacher, and J. A. Nossek, "Multi-array 5g V2V relative positioning: Performance bounds," in *IEEE Global Communications Conference, GLOBECOM 2018, Abu Dhabi, United Arab Emirates, December 9-13, 2018*, 2018, pp. 206–212.

[161] MathWorks, "Dirichlet or periodic sinc function," https://ch.mathworks.com/help/signal/ref/diric.html, [Online; Accessed 20. June 2019].

[162] V. Raghavan, A. Partyka, L. Akhoondzadeh-Asl, M. A. Tassoudji, O. H. Koymen, and J. Sanelli, "Millimeter wave channel measurements and implications for phy layer design," *IEEE Transactions on Antennas and Propagation*, vol. 65, no. 12, pp. 6521–6533, Dec 2017.

[163] L. Koschel and A. Kortke, "Frequency synchronization and phase offset tracking in a real-time 60-ghz cs-ofdm mimo system," in *2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC)*, Sep. 2012, pp. 2281–2286.

[164] S. Ahmadi, "Toward 5 g xilinx solutions and enablers for next-generation wireless systems," 2016.

[165] "Vector Signal Generator," https://www.rohde-schwarz.com/us/manual/r-s-smu200a-vector-signal-generator-operating-manual-manuals-gb1_78701-28893.html, [Online; Accessed 29. November 2019].

[166] "USRP X310," https://www.ettus.com/all-products/x310-kit, [Online; Accessed 29. November 2019].

[167] "mm-wave Setup," https://www.highfrequencyelectronics.com/index.php?option=com_content&view=article&id=1994:affordable-solutions-for-testing-28-ghz-5g-devices-with-your-6-ghz-lab-instrumentation&catid=167&Itemid=189, [Online; Accessed 17. June 2020].

[168] "Mini Circuits," https://www.minicircuits.com, [Online; Accessed 29. November 2019].

[169] "TS-36.104," https://www.3gpp.org/ftp//Specs/archive/36_series/36.104/, [Online; Accessed 12. December 2020].

[170] "MATLAB LTE Toolbox," https://www.mathworks.com/products/lte.html, [Online; Accessed 12. December 2020].

[171] "802.11az," http://www.ieee802.org/11/Reports/tgaz_update.htm, [Online; Accessed 24. September 2019].

[172] A. Ranganathan, B. Danev, and S. Capkun, "Proximity verification for contactless access control and authentication systems," in *Proceedings of the 31st Annual Computer Security Applications Conference*. ACM, 2015, pp. 271–280.

[173] D. Kune, J. Kölndorfer, N. Hopper, and Y. Kim, "Location leaks over the gsm air interface," in *NDSS*, 2012.

[174] M. Gruteser and D. Grunwald, "Enhancing location privacy in wireless lan through disposable interface identifiers: A quantitative analysis," in *Proceedings of the 1st ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots*, ser. WMASH '03. New York, NY, USA: Association for Computing Machinery, 2003, p. 46–55. [Online]. Available: https://doi.org/10.1145/941326.941334

[175] K. B. Rasmussen and S. Čapkun, "Location privacy of distance bounding protocols," in *Proceedings of the 15th ACM conference on Computer and communications security*, 2008, pp. 149–160.

[176] C. Troncoso, M. Payer, J.-P. Hubaux, M. Salathé, J. Larus, E. Bugnion, W. Lueks, T. Stadler, A. Pyrgelis, D. Antonioli, L. Barman, S. Chatel, K. Paterson, S. Čapkun, D. Basin, J. Beutel, D. Jackson, M. Roeschlin, P. Leu, B. Preneel, N. Smart, A. Abidin, S. Gürses, M. Veale, C. Cremers, M. Backes, N. O. Tippenhauer, R. Binns, C. Cattuto, A. Barrat, D. Fiore, M. Barbosa, R. Oliveira, and J. Pereira, "Decentralized privacy-preserving proximity tracing," 2020.