DISS. ETH No. 23319

Physical-layer Techniques for Secure Proximity Verification & Localization

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

Aanjhan Ranganathan

Master of Science in Electrical and Electronic Engineering,
EPFL, Switzerland

born on 07.11.1983

citizen of India

accepted on the recommendation of

Prof. Dr. Srdjan Čapkun, examiner
Prof. Dr. Ivan Martinovic, co-examiner
Prof. Dr. Neal Patwari, co-examiner
Prof. Dr. Mani Srivastava, co-examiner
Prof. Dr. Patrick Tague, co-examiner

2016

What I cannot create, I do not understand.
— Richard Feynmann

dedicated to
my late Gopalan thatha...

Abstract

Today, location and proximity information are key to a number of emerging applications. With the advent of the Internet of Things and autonomous cyber-physical systems, the dependency on location and proximity is likely to increase in the future. Current proximity verification and ranging systems are prone to distance modification attacks that can lead to loss of property (e.g., cars [57]) and even human life (e.g., IMDs [119]). Additionally, GPS which is today the de-facto outdoor localization system is vulnerable to spoofing attacks [76] that forces a receiver to compute a false location. Given the safety and security implications of the applications mentioned above, it is important to ensure the security of the location and proximity estimates used in these systems. Existing solutions based on distance bounding are not suitable for a variety of applications or are not secure against all types of attacks. For example, the design and hardware complexity of current solutions make them unsuitable for contactless access control and authentication systems.

In this thesis, we address these shortcomings and make the following contributions. First, we propose a novel distance bounding system design called Switched Challenge Reflector with Carrier Shifting that enhances existing analog designs to be resilient against strong attackers capable of terrorist fraud. Second, we analyze and enhance a new class of chirp-based ranging solutions that enable the realization of low-power ranging systems. We analyze the security of existing chirp-based ranging systems and demonstrate their vulnerability to distance decreasing relay attacks. We then propose a novel design based on frequency modulated continuous wave (FMCW) and backscatter communication techniques, specifically designed for short-range contactless systems. Finally, in the context of outdoor localization, we present SPREE, the first GPS receiver capable of detecting or mitigating all GPS spoofing attacks described in the literature.

Zusammenfassung

Heutzutage sind Geographische und Näheninformationen der Schlüssel zu einer Reihe von neuen Anwendungen. Mit dem Aufkommen von Internet der Dinge und autonomen Cyber-Physikalischen Systemen, wird sich die Abhängigkeit von Geographischen und Näheninformationen in Zukunft wahrscheinlich erhöhen. Aktuelle Systeme, die die geographische Nähe verifizieren, sind anfällig für Angriffe die die Entfernung verfälschen und dadurch zum Verlust von Eigentum (z.B., cars [57]) und sogar Menschenleben führen können (z.B., IMDs [119]). Zusätzlich ist GPS, der Standard für Außenlokalisierung, anfällig für Spoofing Angriffe [76], die einen Empfänger dazu zwingen eine falsche Position zu berechnen. Angesichts der Zuverlässigkeit und Sicherheitsimplikationen der oben genannten Anwendungen, ist es wichtig sicherzustellen, dass die geographischen Lage und Nähe für diese Systeme zuverlässig bereitgestellt wird. Bestehende Lösungen welche die Distanz feststellen, sind für viele Anwendungen ungeeignet und ebenfalls unsicher gegen viele Arten von Angriffen. Das Design und die Komplexität der Hardware der derzeitigen Lösungen sind zum Beispiel ungeeignet für kontaktlose Zugangskontrollen und Authentifizierungssysteme.

In dieser Doktorarbeit wenden wir uns diesen Mängeln zu und leisten die folgenden Beiträge. Als erstes schlagen wir ein neues Abstands-begrenzungssystem vor names *“Switched Challenge Reflector with Carrier Shifting”*, welches die vorhandenen analogen Designs verbessert, indem es sie robust gegen starke Angreifer macht welche Terror Betrug ausführen können. Zweitens analysieren und verbessern wir eine neue Klasse von chirp-basierten Lösungen, welche energiearme Distanzsysteme ermöglichen. Wir analysieren die Sicherheit von existierenden chirp-basierten Distanzsystemen und zeigen deren Anfälligkeit auf Entfernungsreduktion mittels Relais-attacken. Anschliessend schlagen wir ein innovatives Design vor, welches speziell für Kurzstrecken und kontaktlose Systeme zugeschnitten ist und auf kontinuierlichen frequenzmodulierten Wellen (FMCW) und Backscatter-Kommunikationstechniken basiert. Schlussendlich, präsentieren wir SPREE im Rahmen der Outdoor-Lokalisierung, der erste GPS Empfänger, der alle bekannten GPS Spoofing Angriffe der Literatur mildern oder bekämpfen kann.

Acknowledgments

It is not about the destination. It is about the journey to get there. We are more often fixated in reaching our destination, that we forget to appreciate the journey and the goodness of the people we meet on the way. During the course of my Ph.D., I have acquired life skills and learned numerous lessons that have further enriched my journey towards this doctoral dissertation. I would like to thank all the people who have made this journey memorable with their support, co-operation, understanding, friendship and encouragement.

First and foremost, this journey would not have been possible without the unflinching support of my adviser, Prof. Dr. Srdjan Čapkun. His words of encouragement and motivation especially when the going gets tough, his philosophy as a mentor, his methodology and patience as a teacher are very unique and I consider myself very fortunate to have had him as my doctoral thesis advisor. The freedom he gave to independently explore my own ideas and the confidence he had in my abilities to take a research project to completion were significantly responsible for my development into a researcher. I am very grateful to him for the same.

I would like to thank Prof. Dr. Ivan Martinovic, Prof. Dr. Neal Patwari, Prof. Dr. Mani Srivastava and Prof. Dr. Patrick Tague for consenting to be on my dissertation committee and setting aside time for the review process.

I would like to thank Dr. Boris Danev, Prof. Dr. Aurélien Francillon, and Prof. Dr. Nils Ole Tippenhauer for their invaluable guidance during the initial stages of my doctoral studies. I have learned a lot from them, both technically and in terms of discipline and precision in academic research.

I have made great friends over the course of my studies. Special thanks to Claudio Marforio for all the conversations over numerous beers right from the first day of my doctoral studies. Many thanks to Ramya Masti for patiently listening to all my rants and offering support when it mattered the most. This journey wouldn't have been the same without you folks. I also thank Arthur Gervais for the German translation of the abstract and Dr. Elizabeth Stobert

and Dr. Kari Konstianien for their feedback regarding the dissertation. This journey would be incomplete without the infamous lunchtime discussions with Dr. Claudio Soriente, Dr. Srdjan Marinovic, Dr. Joel Reardon, Nikos Karapanos, Der-Yeuan Yu, Hubert Ritzdorf, Luka Malisa, Arthur Gervais and Hildur Olafsdottir. I am also grateful to Ms. Barbara Pfändner for all the support over the years with administrative matters.

During my stay at the System Security group, I have also had the pleasure of many collaborations. I thank Prof. Dr. Boris Skoric, Dr. Dave Singelée, Prof. Dr. Lothar Thiele, Dr. Devendra Rai and Dr. Frank Gurkaynak for their cooperation and support. I am grateful to the Swiss National Science Foundation for supporting my doctoral studies.

Last but not the least, I extend my gratitude to my family for their unconditional support to the life choices I made. Special thanks to my wife Hajni for her unconditional love, understanding and support, and tolerating my craziness specifically during those never-ending paper submission deadlines. Finally, I would like to dedicate this doctoral dissertation to my late grandpa Gopalan whose joy would have had no bounds seeing me reach this significant milestone in life.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The ability to determine one's own location has been key to human expansion, exploration, and navigation. In ancient times, people relied on far-away light sources, known landmarks or the position of celestial bodies to determine their location and guide them to their intended destinations. Today, with the rapid deployment of wireless systems, a wide variety of new applications depend on location and proximity.

For example, contactless access tokens (e.g., contactless smart/proximity cards, key fobs) are prevalent today in a number of systems including public transport ticketing, parking and highway toll fee collection, payment systems, electronic passports, physical access control and personnel tracking. In a typical access control application, an authorized person simply taps his smart card against a card reader setup at the entrance to gain access to an infrastructure. Smart card-based physical access control and authentication are deployed even in safety- and security-critical infrastructures such as nuclear power plants and defense research organizations. Similarly, in an electronic payment scenario, the consumer places the contactless card in close *proximity* (a few centimeters) to the payment terminal for making secure payments. Furthermore, modern automobiles use passive keyless entry systems (PKES) to unlock, lock or start the vehicle. The vehicle automatically identifies and unlocks when the *key fob* is in close proximity and there is no need for the user to remove the key from his pocket. By removing the need for user interaction, PKES-like systems also offer better protection in scenarios e.g., where the user forgets to manually lock the car. In all the above systems proximity is estimated based on the ability of the contactless access token to communicate with the reader.

Even though the communication range for many such contactless systems is limited to a few centimeters, several works have demonstrated that these radio-frequency based access tokens are vulnerable to relay attacks (NFC phones [58], Google Wallet [121]). In a relay attack, the attacker uses a proxy reader and a proxy card to relay the communications between two legitimate entities without requiring any knowledge of the actual data being transmitted; therefore independent of any cryptographic primitives implemented. Recently, it was shown that the PKES systems used in automobiles are also vulnerable to relay attacks. Researchers were able to unlock the car and drive away even though the legitimate key was several hundred meters away from the car. In addition to relay attacks, an attacker can also modify the measured distance by manipulating the prover's hardware or colluding with other entities. Thus, distance modification attacks have serious implications: an attacker can gain entry into a restricted area, make fraudulent payments or steal a car by simply relaying the communications between the reader and the card which is several meters away without the knowledge of the card's owner.

In order to prevent such distance modification attacks, these systems must be enhanced with distance bounding. Distance bounding guarantees an upper bound on the physical distance between two devices, a verifier, and a prover. Distance bounding was initially introduced in the context of wired systems [33] and later a number of distance bounding protocols [36, 37, 67, 99, 118, 120, 130, 137, 141] were designed for wireless systems. Traditionally, the security of these distance bounding protocols was evaluated by analyzing their resilience against three types of attacks [24, 36, 46]: Distance fraud, mafia fraud, and terrorist fraud attacks. In a distance fraud attack, an untrusted prover tries to shorten the distance measured by the verifier and there is no external attacker involved in the attack. In a mafia fraud attack, an external attacker attempts to shorten the distance measured between an honest and trusted prover and verifier. Terrorist fraud attacks are executed by an untrusted prover who collaborates with an external attacker to convince the verifier that he is closer than he really is.

Although a number of protocol designs have been proposed, there is still a lot of scope for improving the state of the art with respect to the actual realization of these systems. For example, Tippenhauer et al. [136] designed one of the first distance bounding systems based on ultra-wideband impulse radio ranging. However, the hardware requirements of the design (e.g., sampling rate) make it infeasible for applications such as contactless payments where low hardware complexity is a key requirement. Other distance bounding designs such as [118] have limited compatibility with higher level protocols (e.g., majority of distance bounding protocols proposed in literature cannot be implemented using this design). Furthermore, they do not protect against all types of distance bounding attacks.

In addition to proximity, the exact location is critical to a large number of applications ranging from navigation and tracking to modern communication and networking systems. Furthermore, there is an increasing number of autonomous cyber-physical systems (e.g., drones and self-driving cars) that rely on accurate location estimates for their positioning and navigation. In outdoor scenarios, the Global Positioning System (GPS) is the de-facto method for determining one's location today. GPS is a satellite-based navigation system in which the receiver on the ground estimates its location based on the messages received from the satellites. The messages are transmitted using publicly available codes and lack any form of authentication. Therefore, GPS is vulnerable to signal spoofing attacks in which an attacker transmits specially crafted signals that overshadow authentic satellite signals, forcing the receiver to compute a false location. Researchers recently demonstrated the insecurity of GPS-based navigation by diverting the course of a yacht using spoofed GPS signals [13]. Similarly, using fake GPS signals, they demonstrated how to hijack a drone and force it to land at any pre-determined location. Furthermore, these attacks were carried out using devices that cost less than $1000. Existing countermeasures that detect or mitigate GPS spoofing attacks are either ineffective against strong attackers or are not reliable enough to distinguish spoofing attacks from real-world signal effects. Even with cryptographic authentication, the system is not protected against relay attacks where an attacker simply records and replays the radio signals to the receiver [106].

The set of applications using location and proximity is only bound to increase especially given the recent advent of Internet of Things (IoT). Thus, there is a need to ensure the resilience of these systems against modern day cyber-physical attacks.

1.1 Contributions

As described previously, even though a number of distance bounding protocols are present in literature, very few practical realizations exist. Furthermore, the proposed solutions are not suitable for a variety of applications or are not secure against all types of attacks. For example, it has been shown that implementing distance bounding using analog processing techniques provides tighter security guarantees than digital implementations. However, existing analog implementations do not support resilience against Terrorist Fraud attacks; they are only suited for the prevention of Distance Fraud and Mafia Fraud attacks. Also, the design and hardware complexity of current distance bounding systems make them unsuitable for certain applications such as contactless access control and authentication systems. Furthermore, GPS, which is today the de-facto system used for outdoor localization is vulnerable to spoofing attacks. There is currently no GPS receiver that is resilient against all known GPS spoofing attacks. In this thesis, we address the drawbacks mentioned above and make the following contributions.

Terrorist fraud resilient distance bounding system: We propose a novel, hybrid digital-analog design called *Switched Challenge Reflector with Carrier Shifting* that enables the implementation of terrorist fraud resilient distance bounding protocols. Furthermore, we introduce a new attack, which we refer to as the *double read-out* attack and show that our proposed system is also secure against this attack. Our system consists of a prototype prover that provides strong security guarantees: if a dishonest prover performs the terrorist fraud attack, it can cheat on its distance bound to the verifier only up to 4.5 m and if it performs Distance Fraud or Mafia Fraud attacks up to 0.41 m. We show that our system can be used to implement existing (terrorist fraud resilient) distance bounding protocols without requiring protocol modifications.

Even though the above-proposed design mitigates all known distance bounding attacks, the design requirements are still complex and not suitable for applications such as contactless access control systems. Therefore, we look into a new class of emerging ranging systems, analyze its security properties and propose a novel architecture specifically designed for use in contactless systems. Specifically, we make the following contributions:

Security analysis of chirp-based ranging systems: Ultra-wideband (UWB) and Chirp Spread Spectrum (CSS) are emerging as the most prominent techniques for short and medium distance localization. In contrast to UWB-IR, the physical characteristics of chirp signals allow low-complexity and low-power realization of both communication and ranging systems [103]. In this thesis, we analyze the vulnerability of Chirp Spread Spectrum (CSS) based ranging and localization systems. Specifically, we demonstrate the feasibility of distance decreasing relay attacks that have proven to be detrimental to the security of proximity-based access control systems (e.g., passive vehicle keyless entry and start systems, contactless cards). We show that an attacker is able to effectively reduce the measured distance by almost 700 m depending on the chirp configuration. We discuss possible countermeasures in order to prevent these attacks.

Secure Proximity Verification for Contactless Systems: Motivated by the findings of the above security analysis, we propose a novel distance bounding system specifically designed for short-range contactless access control and authentication applications. Our system combines frequency modulated continuous wave (FMCW) and backscatter communication. The use of backscatter communication enables low-complexity, power-efficient design of the prover which is critical for contactless smart cards. In addition, our distance bounding system enables the implementation of a majority of distance bounding protocols developed in prior art. We analyze our system in various attack scenarios and show that it offers strong security guarantees. Additionally, we evaluate our system's communication and distance measurement characteristics using a prototype implementation.

Spoofing Resistant GPS Receiver: In addition to proximity, several applications such as navigation and tracking, communication and networking infrastructures rely on location information. Currently, wide-area localization infrastructures that use distance bounding to provide secure location estimates do not exist and GPS is today the most prevalent method of estimating location outdoors. However, as mentioned before, GPS is vulnerable to signal spoofing attacks. Therefore, it is necessary to build a GPS receiver that is resilient against spoofing attacks. In this thesis, we present SPREE, which is, to the best of our knowledge, the first GPS receiver capable of detecting or mitigating all GPS spoofing attacks described in the literature. In SPREE, we introduce a novel spoofing detection technique, which we refer to as auxiliary peak tracking, that limits even the strongest attacker known in the literature (seamless takeover attack) from spoofing the receiver to an arbitrary location. We combine auxiliary peak tracking with existing GPS countermeasures and show how their combination results in an even more reliable detection. We implement and evaluate our receiver against the de-facto standard of a publicly available repository of GPS signal traces. We further evaluate SPREE against our own dataset obtained through extensive wardriving and commercial GPS simulators. Finally, we release our implementation and dataset to the community for further research and development [11].

1.2 Thesis Organization

The thesis is organized as follows. We begin the thesis with an overview of existing ranging systems, their vulnerability to distance modification attacks and the existing solutions in Chapter 2. Chapter 3 describes the design of our "Switched Challenge Reflector with Carrier Switching" prover. First, we give a brief overview of existing terrorist fraud resilient protocols and motivate our prover's design. We then describe its design and evaluate its effectiveness against all distance bounding attacks known in the literature.

In Chapter 4, we investigate physical-layer distance decreasing attacks on CSS-based ranging systems. In this chapter, we provide an overview of Chirp Spread Spectrum and discuss the attacks that can be mounted on chirp-based ranging systems. Then, we evaluate the feasibility of the attacks through experiments and discuss the implications of our findings. We conclude the chapter by enumerating possible countermeasures and describing related work.

In Chapter 5, we first motivate the importance of developing low-complexity, power-efficient distance bounding systems. We propose a novel distance bounding system with a ranging precision and security guarantees suited for contactless access control and authentication applications. We describe a complete system architecture and show that it provides complete protection against conventional distance modification attacks. Finally, we evaluate our system through simulations and experimentally validate its processing delay, power consumption and ranging precision.

Finally, in Chapter 6, we present the design of SPREE, the first GPS receiver capable of detecting all known GPS spoofing attacks. We begin this chapter with a brief overview of GPS, a typical GPS receiver's hardware architecture, and its operation. We then classify the various types of GPS spoofing attacks and discuss why state-of-art countermeasures fail. Then, we describe our proposed GPS receiver's design and its main features. Finally, we evaluate our receiver against a variety of adversarial and non-adversarial scenarios and present the results.

We conclude the thesis in Chapter 7 with a summary of our findings and present possible future work.

1.3 Publications

Parts of this thesis are based on the following articles I have co-authored.

- Aanjhan Ranganathan, Boris Danev, Srdjan Capkun, Proximity Verification for Contactless Access Control and Authentication Systems, *In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC 2015)*

- Aanjhan Ranganathan, Nils Ole Tippenhauer, Boris Skoric, Dave Singelée, Srdjan Capkun, Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System, *In Proceedings of 17th European Symposium on Research in Computer Security (ESORICS 2012)*

- Aanjhan Ranganathan, Boris Danev, Aurélien Francillon, Srdjan Capkun, Physical-layer attacks on chirp-based ranging systems. *In Proceedings of the 5th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC 2012)*

- Aanjhan Ranganathan, Hildur Ólafsdóttir, Srdjan Capkun, SPREE: Spoofing Resistant GPS Receiver, *arXiv preprint 1603.05462 (2016)*

In addition, during my Ph.D., I co-authored the following publications.

- Ramya Jayaram Masti, Devendra Rai, Aanjhan Ranganathan, Christian Müller, Lothar Thiele, Srdjan Capkun, Thermal Covert Channels on Multi-core Platforms, *In the proceedings of 24th USENIX Security Symposium (USENIX Security 15)*

- Nils Ole Tippenhauer, Luka Malisa, Aanjhan Ranganathan, Srdjan Capkun, On Limitations of Friendly Jamming for Confidentiality, *In Proceedings of IEEE Symposium on Security and Privacy 2013 (IEEE S&P 2013)*

- Ramya Jayaram Masti, Claudio Marforio, Aanjhan Ranganathan, Aurélien Francillon, Srdjan Capkun, Enabling Trusted Scheduling in Embedded Systems, *In Proceedings of the 28th Annual Computer Security Applications Conference (ACSAC 2012)*

Chapter 2

Ranging Systems and Distance Bounding

2.1 Introduction

The widespread deployment of wireless systems that use location and proximity to provide services has led to the advent of many radio frequency based ranging and localization technologies [91]. Today, these systems are used in a broad set of scenarios including people and asset tracking, emergency and rescue support [54] and access control [62, 119]. Numerous ranging and localization technologies were developed in the last decade [91]; they differ in communication channels (e.g., radio frequency, optical), position-related parameters (e.g., received signal strength (RSS), time-of-arrival (TOA), time-difference-of-arrival (TDOA)), target operating environment (e.g., indoor, outdoor), precision and reliability. Prominent examples include GPS [96] for outdoor localization and systems based on RSS [22, 154], TDOA [142, 156] and round-trip time-of-flight (RTOF) [14, 145] operating both outdoors and indoors. Most of these distance measurement techniques are inherently insecure. For example, an attacker can fake the signal strength in an RSS based distance measurement system. Similarly, in an ultrasonic ranging system, an attacker can gain advantage by relaying messages over the faster RF channel [127].

Given the safety and security implications of the applications mentioned above, it is important to ensure secure distance and location estimation in these systems. Distance bounding enables the secure measurement of an upper bound on the physical distance between two devices, a verifier and a prover, even if the prover is untrusted and tries to reduce the measured distance. Distance bounding was initially introduced in the context of wired systems [33] and later a number of distance bounding protocols [36, 37, 67, 99, 118, 120, 130, 137, 141] were designed for wireless systems. In order to compute the upper bound on the physical distance, distance bounding relies on the measurement of the round-trip time between a transmitted challenge and a received response. Successful execution of a distance bounding protocol relies on two main assumptions: (i) Precise distance bound estimate and (ii) Low processing time at the prover to compute the response. Precise measurement of the distance depends largely on the physical characteristics of the RF signal and the time-of-arrival estimation technique implemented in the system. The time taken by the prover to process the challenge (i.e., demodulate, compute and transmit the response) depends on the chosen processing function and is therefore critical to prevent distance modification attacks such as distance fraud [33] or mafia fraud [46]. Reducing this processing time is therefore critical, such that the prover cannot modify its processing time arbitrarily and pretend to be closer to the verifier. Therefore, one line of work focussed on designing fast provers using only analog processing techniques [118] to reduce the prover processing time to less than a nanosecond. Another line of work took the conventional approach of implementing distance bounding using ultra-wide band (UWB) signals with well defined physical-layer characteristics.

In this chapter, we provide a brief overview of radio frequency based ranging techniques and describe their vulnerabilities to distance modification attacks. Then, we introduce the concept of distance bounding and discuss the different attacker models used in their security analysis. Finally, we present the state of the art with respect to the design and implementation of distance bounding systems and discuss their limitations.

2.2 Security Analysis of Modern Ranging Systems

The rapid deployment of wireless systems has driven an increasing interest in the use of radio communication technologies for ranging and localization [25]. Ranging and localization are two closely related concepts. Ranging is the method used to determine the physical distance between two entities while localization is the process of computing an exact position or geographic co-ordinate of an entity. Commonly used localization techniques such as multilateration rely on multiple distance measurements to compute the location of an entity. In fact, GPS, the most popular outdoor localization technology uses multilateration to compute the location. Thus, distance measurement is a fundamental first step in a majority of modern localization and positioning systems.

Numerous ranging techniques that use radio communication signals have been developed in the recent years. We classify these ranging techniques broadly into two categories: (i) Indirect ranging – techniques that determine distance by measuring one or more physical properties (e.g., amplitude, phase and frequency) of the signal, (ii) Direct ranging – techniques that compute distance based on the signal's time of flight and its speed of propagation. Techniques that compute distance based on the signal's physical properties such as received signal strength, multicarrier phase ranging, frequency modulated continuous wave radars can be classified as indirect ranging techniques. Ranging techniques that rely on measuring round-trip time of flight, time of arrival, time difference of arrival can be categorized as direct ranging techniques. In the following section, we describe the ranging techniques mentioned above in more detail and discuss their vulnerability to distance modification attacks.

Throughout this thesis, we refer to the entity that computes the distance as the verifier and the entity whose distance is estimated as the prover. We assume a Dolev-Yao attacker [47] with the capability to eavesdrop, modify, compose, and (re)play any messages transmitted and received by the verifier and the prover. In the context of ranging systems, the goal of an attacker is to force the verifier to compute a false verifier-prover distance by manipulating the signals transmitted and received by the two entities.

2.2.1 Indirect Ranging Techniques

In this section, we review the vulnerability of ranging systems that compute distances based on the signal's physical characteristics such as amplitude (RSS), phase (multicarrier phase ranging) or frequency (FMCW).

Received signal strength: Received signal strength (RSS) [22, 35, 60, 71, 114, 126, 152] based ranging systems rely on the free space path loss propagation model to estimate the distance between the verifier and the prover. Any radio signal experiences a loss in its signal strength as it travels through space. The amount of loss or attenuation in the signal's strength is proportional to the square of the distance between the transmitter and the receiver. Mathematically, the exact distance d is calculated based on the following free space path loss equation:

$$d = \frac{\lambda}{4\pi}\sqrt{\frac{P_t G_t G_r}{P_r}} \tag{2.1}$$

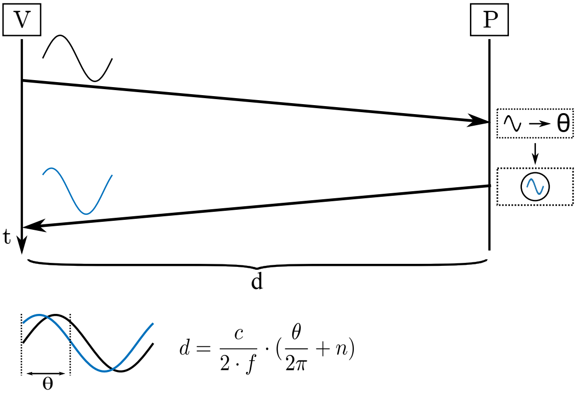


Figure 2.1: *The prover locks its local oscillator to the verfier's signal and transmits it back to the verifier. The verifier then measures the distance based on the difference in the phase of the received signal and its own reference signal.*

where λ is the signal's wavelength, P_t and P_r are the transmitted and 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 tall buildings) which are difficult to account for accurately. This directly affects the accuracy of the computed distance. Advanced models such as the Rayleigh fading and log-distance path loss models [116] are typically used to improve the distance estimation accuracy.

Attacks: In an RSS-based ranging system, an attacker can trivially cheat on the measured distance by faking the received signal strength at the verifier. For example, the attacker can simply attenuate or amplify the signal transmitted by the prover before relaying it back to the verifier. This will result in the verifier estimating a false or incorrect distance to the prover. Also, a dishonest prover can cheat by transmitting the signal at a different power level than what is specified or used by the verifier to estimate the distance.

Multicarrier phase ranging: In phase-based ranging, two devices measure the distance between them by estimating the phase difference between a received continuous wave signal and a local reference signal. For example, if the verifier V is measuring its distance to a prover P, then the verifier begins ranging by transmitting a continuous wave carrier signal. The prover locks its local oscillator to this incoming signal and transmits it back to the verifier. The verifier measures the distance based on the difference in the phase of the received signal and its own reference signal as shown in Figure 2.1. If the distance d between the verifier and the prover is less than the signal's wavelength i.e., $\frac{2 \cdot f}{c}$, where f is the frequency of the signal and c is the speed of light, the measured phase difference θ will be,

$$\theta = 4\pi \cdot \frac{d \cdot f}{c} \tag{2.2}$$

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. Therefore, the equation for measuring d becomes,

$$d = \frac{c}{2 \cdot f} \cdot (\frac{\theta}{2\pi} + n) \tag{2.3}$$

where n is an integer which reflects the number of whole cycles elapsed. The need for keeping track of n is eliminated by using continuous wave signals of different frequencies.

Multicarrier phase ranging systems [10,21,50,95,124,157] eliminates the whole cycle ambiguity by transmitting continuous wave signals at different frequencies (Figure 2.2). For example, the verifier first transmits a signal with a frequency f_1 to which the prover locks its local oscillator and retransmits the signal back to the verifier. At the verifier, the measured phase difference between the received signal from the prover and the verifier's own signal for this frequency (θ_1) is given by (from Equation 2.3),

$$\theta_1 = 2\pi \cdot (\frac{2 \cdot d \cdot f_1}{c} + n) \tag{2.4}$$

The verifier then transmits a continuous wave signal with a frequency f_2 and measures the phase difference (θ_2) as previously.

$$\theta_2 = 2\pi \cdot (\frac{2 \cdot d \cdot f_2}{c} + n) \tag{2.5}$$

The distance d between the verifier and the prover can be unambiguously measured by combining equations 2.4 and 2.5:

$$d = \frac{c}{4\pi} \cdot \frac{\theta_2 - \theta_1}{f_2 - f_1} \tag{2.6}$$

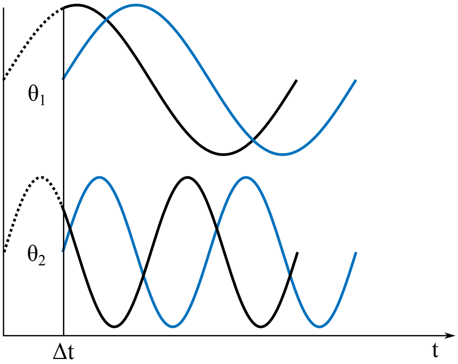


Figure 2.2: *Two signals of different frequency that travel the same amount of time will experience a different phase shift.*

In this case, the maximum distance that can be measured depends on the difference between the two frequencies after which the measured distance rolls over to zero. Frequency hopping spread spectrum techniques are typically used to improve the accuracy of the estimated distance. The size of the frequency hop then decides the maximum measurable distance [25].

Attacks: The maximum measurable distance i.e., the largest value of distance d_{max} that can be estimated using multicarrier phase-ranging system, depends on the maximum measurable phase difference $\Delta\theta_{max}$ between the two frequency signals. Given that the phase values range from 0 to 2π, the maximum measurable phase difference between any two frequencies is $\Delta\theta_{max} = 2\pi$. Substituting the values in Equation 2.6, the maximum measurable distance is given by,

$$\begin{aligned} d_{max} &= \frac{c}{4\pi} \cdot \frac{\Delta\theta_{max}}{\Delta f} \\ d_{max} &= \frac{c}{2} \cdot \frac{1}{\Delta f} \end{aligned} \tag{2.7}$$

For example, if the frequency hop size is 2 MHz (Δf), the maximum distance measurable without any ambiguity is 75 m after which the measured distance rolls over to 0 m. Similarly for frequency hop sizes of 0.5, 1, 2, 4 MHz, the maximum measurable distances are 300, 150, 75 and 37.5 m respectively.

An attacker can leverage the maximum measurable distance property of the ranging system in order to execute the distance decreasing relay attack. During the attack, the attacker simply relays (amplify and forward) the verifier's interrogating signal to the prover. The prover determines the phase of the interrogating signal and re-transmits a response signal that is phase-locked with the verifier's interrogating signal. The attacker receives the prover's response signal and forwards it to the verifier, however with a time delay (Δt). The attacker chooses the time delay such that measured phase differences $\Delta\theta$ between the carrier frequency signals reaches its maximum value of 2π and rolls over. Considering the previous example of a system with the frequency hop size of 2 MHz, the measured phase differences $\Delta\theta$ rolls over every $500\,\text{ns}$. Additionally, a stronger attacker can receive the signal from the prover and shift the signal's phase before relaying back to the verifier. The attacker shifts the phase of the signal such that it results in the verifier computing an appropriate false distance.

Frequency modulated continuous wave: FMCW radars use chirp signals [26] to determine range and velocity of a target (here the prover). The verifier transmits an interrogating chirp signal i.e., a continuous wave signal with a linearly increasing or decreasing frequency. The prover receives and reflects this signal back to the verifier. The reflected signal is then mixed at the verifier with the transmitted signal at that instant to produce a *beat signal*. The frequency of the beat signal is proportional to the round-trip time taken to receive the reflected chirp signal; thereby able to measure distance d to the prover. The distance d is estimated using the equation:

$$d = \frac{c \cdot f_{\Delta} \cdot T_s}{2 \cdot f_{bw}} \tag{2.8}$$

where c is the speed of light, f_{Δ} is the frequency of the beat signal, f_{bw} is the total bandwidth of the chirp signal and T_s indicates the time period of the chirp signal. We present a more elaborate explanation of FMCW in Chapter 5.

Attacks: An attacker can manipulate the estimated distance in several ways. For instance, the attacker can shift the frequency of the reflected signal before relaying it back to the verifier. This would result in a different beat signal frequency, and therefore a false distance estimate at the verifier. In systems where the verifier continuously transmits interrogation signals, then an attacker can also manipulate the estimated distance by executing a *rollover* attack similar to the one presented for phase-based ranging systems. An attacker would then have to simply delay the prover's reflected signal longer than the time duration of one interrogating chirp signal. The delayed signal is then mixed with a *successive* interrogation signal resulting in a different beat frequency and therefore a false distance estimate at the verifier.

Thus, from the above discussions we may conclude that ranging techniques that solely rely on estimating distance as a function of the variations in the signal's amplitude, phase or frequency is vulnerable to distance modification attacks.

2.2.2 Direct Ranging using Time of Flight

An alternative approach for estimating distance is by measuring the time taken for the signal to travel from the verifier to the prover. Knowing the propagation speed of the radio signal (approximately close to the speed of light), the distance d between the verifier and the prover can be mathematically expressed using the equation

$$d = (t_{rx} - t_{tx}) \cdot c \tag{2.9}$$

where c is the speed of light, t_{tx} and t_{rx} represent the time of transmission and reception respectively.

In addition to the precise knowledge of the transmission and reception times, the time-of-fight measurement requires tight clock synchronization between the verifier and prover. Note that, a 1 ns error in synchronization would result in ≈ 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. The round trip time is the time elapsed between transmitting a ranging data packet and receiving an acknowledgment back from the prover. The distance between the verifier and the prover is then given by the equation:

$$d = \frac{c.(t_{RTT} - t_p)}{2} \tag{2.10}$$

where c is the speed of light ($3 \cdot 10^8$ m/s), t_{RTT} is the measured round-trip time and t_p is the processing delay i.e., the time taken by the prover to receive, process and transmit the acknowledgment back to the verifier. This type of ranging is often referred to as two-way time-of-flight ranging and mitigates the requirement for tight clock synchronization between the verifier and the prover.

Thus, precise distance measurement largely depends on the time-of-arrival estimation technique implemented in the system and the physical characteristics of the radio frequency signal itself. As a general rule of thumb, the ranging resolution is directly proportional to the bandwidth of the ranging signal [131]. Today, ultra-wideband (UWB) and chirp spread spectrum (CSS) are emerging as the most prominent physical-layer for modern precision ranging systems [16,44,45,103,113] due to their high bandwidth and resilience against multipath and other channel disturbances. As mentioned previously, time of flight is typically calculated by measuring the time elapsed between transmitting a ranging data packet and receiving a corresponding acknowledgment back from the prover. UWB Impulse Radio (UWB-IR) [16,44,45,113] based ranging systems use short duration pulses (typically $2-3$ ns long) to transmit ranging and acknowledgment packets. CSS-based ranging systems [103] modulate the ranging data using up- and down-chirp signals.

Attacks: Regardless of the physical layer (i.e., whether UWB or CSS is used for ranging), an attacker can manipulate the time-of-flight measurements and thus the estimated distance. The majority of the time-of-flight ranging systems use pre-defined data packets for ranging, making it trivial for an attacker to predict and generate his own ranging or acknowledgment signal. For example, an attacker can transmit the acknowledgment packet even before receiving the challenge ranging packet. Flury et al. [56] showed that the de facto standard for IR-UWB, IEEE 802.15.4a [77], does not automatically provide security against distance decreasing attacks. It was shown that an external attacker can potentially decrease the measured distance by as much as 140 meters by predicting the preamble and payload data with more than 99% accuracy even before receiving the entire symbol. Similarly, Poturalski et al. [109] introduced the Cicada attack on the impulse radio ultra wide-band physical layer. In this attack, a malicious transmitter continuously transmits a “1” impulse with a power greater than that of an honest transmitter. This degraded the performance of energy detection based receivers, resulting in reduction of the distance measurements. In Chapter 4, we evaluate the security of CSS-based ranging systems to such physical-layer attacks. Furthermore, some commercial ranging systems [44, 103] allow the prover to communicate the time taken to process the verifier’s challenge signal. In such a scenario, a dishonest prover can trivially cheat on the distance by either reporting a false signal processing time delay or by actually manipulating the time taken to process the signal itself (e.g., using specialized hardware).

To summarize, both indirect and direct ranging techniques are vulnerable to distance modification attacks. Indirect ranging techniques (e.g., based on

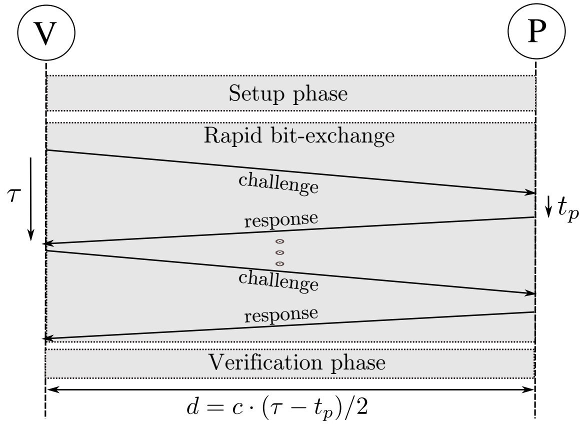


Figure 2.3: *The three phases of a distance bounding protocol. (i) Setup phase where specific information is exchanged between the prover and the verifier, (ii) Rapid-bit exchange where single bit challenges and responses are exchanged and (iii) Verification phase where the responses are validated and distance bound is estimated.*

received signal strength, phase or frequency) can be trivially manipulated by faking the amplitude, phase or frequency of the radio signal. Direct ranging techniques estimate distance based on the time elapsed between sending a ranging packet and receiving a corresponding acknowledgment. The security of direct ranging systems depend on a number of factors such as the data exchanged during the ranging process, the modulation technique used etc. For example, it is important that the verifier and the prover exchange data that is cryptographically generated. Otherwise, it would be trivial for an unauthorized device to recreate the ranging signals and appear legitimate to the verifier. In short, in order to prevent distance modification attacks, it is not only necessary to exchange data but it has to be coupled with the distance estimation method in a way that prohibits modification or relaying.

2.3 Distance Bounding

In this section, we introduce the concept of distance bounding and give an overview of its state of the art implementations. The concept of distance bounding was first proposed by Brands and Chaum [33]. The goal of a distance bounding system is that a verifier establishes an upper bound on its physical distance to a prover. Distance bounding protocols follow a specific procedure which typically includes a setup, rapid-bit exchange and verification phases (Figure 2.3). In the setup phase, the verifier and the prover agree or commit to specific information that will be used in the next protocol phases. In the rapid-bit exchange phase, the verifier challenges the prover with a number of single-bit challenges to which the prover replies with single-bit responses. The verifier measures the round-trip times of these challenge-reply pairs in order to estimate the verifier's upper distance bound to the prover. The distance d between the verifier and the prover is calculated using the equation

$$d = \frac{c.(\tau - t_p)}{2} \tag{2.11}$$

where c is the speed of light ($3 \cdot 10^8\,\mathrm{m/s}$), τ is the round-trip time elapsed and t_p is the processing delay at the prover before responding to the challenge. The verification phase is used for confirmation and authentication. It should be noted that depending on the protocol construction the verification phase may not be required.

The security of distance bounding protocols is traditionally evaluated by analyzing their resilience against three types of attacks: *Distance fraud*, *mafia fraud* and *terrorist fraud* attacks. Figure 2.4 shows these attack scenarios and the entities involved. In a *distance fraud attack*, an untrusted prover tries to shorten the distance measured by the verifier. Since the round-trip time includes the processing delay, an untrusted prover can reduce the distance measured by either sending its replies before receiving the challenges or by computing the responses faster. There is no external attacker involved in this attack.

Mafia fraud attacks, also called relay attacks, were first described by Desmedt [46]. In this type of attack, both the prover and verifier are honest and trusted. An external attacker attempts to shorten the distance measured between the prover and the verifier by relaying the communications between the entities. Distance bounding protocols prevent relay attacks due to the fact that the time taken to relay the challenges and responses will only further increase the distance bound estimate. However, it is important to keep the variance of the prover's processing time to a minimum to ensure high-security guarantees. If the time taken by the prover to process challenges varies significantly between challenges, the verifier has to account for the high variance in its distance estimation. Depending on the amount of variance to be accounted for, an attacker can reduce the distance by relaying communications between the prover and the verifier.

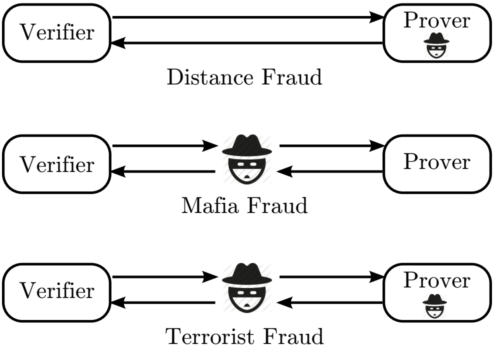


Figure 2.4: *Attacks on distance bounding systems. In distance fraud, an untrusted prover tries to cheat on the measured distance. Mafia fraud is achieved by an external attacker by relaying information between a trusted prover and verifier. In terrorist fraud, the prover colludes with an external attacker to cheat on the measured distance.*

Finally, in *terrorist fraud attacks* [24], an untrusted prover collaborates with an external attacker to convince the verifier that the prover is closer than its true distance. All countermeasures to terrorist fraud make the assumption that the untrusted prover does not reveal his long-term (private or secret) key to the external attacker which he collaborates with.

Recently, another type of attack on distance bounding protocols called the *distance hijacking* attack was proposed [41]. The authors give a real world example of a dishonest prover with a stolen smart card gaining access to a secure facility; though he is not within the required proximity. The attacker exploits an honest prover's presence by hijacking its rapid bit-exchange phase with the verifier. As demonstrated in [41], a system's resilience to distance hijacking depends on the higher level protocol implementation and is independent of the physical-layer.

2.4 Distance Bounding Implementations

A number of distance bounding protocols [29–31, 36–38, 59, 67, 70, 81, 87, 99, 105, 118, 120, 129, 130, 137, 141, 144] were proposed following the work of Brands and Chaum [33]. These protocols provide resilience against one or all of the attacks mentioned above. However, the security of these protocols are mostly analyzed based on information-theoretic proofs without considering physical layer attacks. For example, a protocol is said to be resilient against distance fraud attacks if the response bits are dependent on the challenge bits, i.e., the prover cannot respond before actually receiving the challenge. As described previously, a prover's distance is measured based on some physical layer parameter such as received signal strength or round trip times. Therefore, in practice, the security of distance bounding protocols also depends on the actual physical layer design and implementation of the distance bounding system.

For instance, an untrusted prover can use specialized or modified hardware to compute a response faster than the delay expected by the verifier to estimate the distance. It is important to note that a speedup of 1 ns translates to a distance gain of approximately 15 cm[1] . An attacker can also reduce the distance between the verifier and prover by detecting or demodulating challenges before receiving them completely or late committing a response as shown by Clulow et al. [39]. In order to address these attacks specific to the physical layer, the research focus shifted towards secure physical layer design of distance bounding systems.

Initial distance bounding implementations [117, 125] proposed the use of both radio frequency and ultrasound. The verifier that wants to securely verify the location claim of a prover transmits a challenge using RF and the prover responds back using ultrasound. Based on the time-of-arrival of the ultrasound packet, the location claim l of the prover, and the propagation time of radio and ultrasound signals in the air, the verifier estimates the prover's distance d. If d is larger than the claimed distance l, the verifier rejects the prover's location claim. The use of RF communication in both directions would make the prover's processing delay very large, and thus making the system unusable. One of the main problems with these systems is that an untrusted prover or an external attacker with a proxy node in the verifier's region of interest can take advantage of this. By using radio frequency as a wormhole channel to echo the response back to the verifier, the attacker can reduce the round-trip-time and hence the distance estimate. Hence, it became essential to develop new radio frequency-based distance bounding systems.

RFID Distance Bounding Channel: Hancke et al. [67] introduced one of the first distance bounding protocols and subsequently extended this work further with a UWB communication channel [65]. In the proposed channel, the verifier embeds the challenge bits as ultra-wideband pulses in addition to the transmitted carrier signal. These pulses are transmitted with a delay after every rising edge of the carrier signal. This delay is known apriori to both the

[1] based on the distance traveled by light in 1 ns

verifier and the prover. The presence or absence of the pulse indicates whether the challenge bit is 1 or 0. The prototype implementation resulted in distance bounds for near field RFID up to 1 m for trusted provers and 11 m in the case of untrusted provers. Several challenges exist in implementing this design. First, since the communication link includes both low-frequency carrier and the ultra-wideband pulses, the complexity of the RFID tag's receiver architecture increases. Second, the ambiguity in the distance still depends on the processing delay of the prover. Hence, an untrusted prover with access to faster hardware can reduce the processing delay thereby cheating on the distance estimated by the verifier.

UWB-IR Distance Bounding System: Tippenhauer et al. [136, 138] designed and implemented a distance bounding system with a focus on optimizing the rapid bit-exchange phase. Due to the ranging precision and resilience to multipath effects, an ultra-wideband impulse radio (UWB-IR) physical layer was used for communication. UWB-IR systems communicate data using short pulses which are typically $2-3$ ns long. Range estimation is based on the time elapsed between transmitting a challenge pulse and receiving a corresponding response. In any distance bounding protocol the rapid bit-exchange phase is the core and the final distance estimation is based on the exact timing of these challenge and response pulses. Since the design primarily focused on the fast rapid bit-exchange phase, any distance bounding protocol can be implemented and deployed using this system. The processing delay at the prover depends on the protocol adopted e.g., the XOR processing function used in the prototype implementation resulted in an overall delay of ≈ 100 ns. However, the narrow UWB-IR pulses utilize a large bandwidth (> 500 MHz) which require both the prover and the verifier to be equipped with high sampling rate analog-to-digital (ADC) and digital-to-analog converters (DAC) to receive and transmit UWB-IR pulses respectively.

Challenge Reflection with Channel Selection (CRCS): The design focussed primarily on reducing the prover's processing delay to a minimum. In this regard, CRCS [118] took an unconventional approach and reduced the prover's processing delay to 1 ns. This was achieved by eliminating the need for interpreting the challenge during the rapid-bit exchange phase. In this design, the prover commits to a precomputed nonce during the initialization phase. In the rapid-bit exchange phase, the verifier transmits the challenge signal to the prover. In contrast to traditional distance bounding designs, in CRCS, the prover simply reflects the challenges back to the verifier on dif-

Implementation	Attack Resilience			Compatible Protocols	Complexity[b]
	DF (processing delay)[a]	MF	TF		
UWB-IR [136]	✓ (100 ns)	✓	✓	Any	High
RFID DB Channel [65]	✓ (40 ns)	✓	×	HKP [67]	High
CRCS [118][c]	✓ (1 ns)	✓	×	CRCS	High

[a] A 1 ns prover processing delay enables a maximum distance reduction of 15 cm by a dishonest prover.

[b] Required signal sampling rates, memory etc..

[c] Focused primarily on reducing the prover's processing delay and used frequency switching to communicate data.

Table 2.1: *Comparison of the existing distance bounding implementations in prior work.*

ferent frequency channels. The frequency channel on which the challenge signals are reflected depends on the prover's pre-computed nonce. Since the prover does not demodulate the challenge, compute and then transmit back the response during the time critical rapid-bit exchange phase, it was possible to achieve a net processing delay of less than a nanosecond at the prover. However, given that the incoming challenge is not interpreted during the time-critical phase, the majority of state-of-art distance bounding protocols (e.g., Brands-Chaum [33], Hancke-Kuhn [67]) cannot be realized using this scheme. In addition, the lack of challenge demodulation makes this scheme vulnerable to terrorist fraud attacks. For example, an untrusted prover can pre-calculate the responses (since they are independent of the challenge signal in CRCS) and forward them to a colluding attacker located near the verifier. The colluding attacker can then successfully execute the rapid-bit exchange phase with the verifier. In addition, the absence of challenge interpretation during the rapid-bit exchange phase makes the system vulnerable to simple response replay attacks. In order to prevent such attacks, the prover needs to demodulate, store and communicate the challenges back to the verifier during the final verification phase of the protocol.

2.5 Summary

All existing ranging systems are vulnerable to distance modification attacks. In order to secure them, it is important to enhance modern ranging systems with distance bounding. Currently, the design and development of distance bounding systems follow two approaches. One set of designs such as the UWB-based distance bounding systems [65, 136, 138] took a more conventional approach to designing distance bounding systems and used ultra-wide band signals as the physical layer. In these designs, the challenges are received, decoded and the appropriate response is computed during the time-critical rapid-bit exchange phase. Although this enabled the realization of the majority of distance bounding protocols, the prover's processing delay was still on the order of one hundred nanoseconds. This means that an untrusted prover with specialized hardware could easily modify the estimated distance by speeding or slowing the computation of the response signal. Another approach to realizing distance bounding is to eliminate the need for demodulation and computation of response signals during the rapid-bit exchange phase of the protocol [118]. Such an approach results in fast prover designs, but due to the lack of challenge interpretation during the bit-exchange phase, the majority of distance bounding protocols proposed in the literature cannot be implemented. For example, terrorist fraud resilient distance bounding protocols require the prover to generate the responses based on the received challenges. The absence of challenge interpretation at the prover allows a dishonest prover to collude with an external attacker who is in close proximity to the verifier (e.g., communicating the responses to the attacker even before receiving the challenges) and successfully execute the distance reduction attack.

Furthermore, all existing distance bounding designs require specific hardware requirements at the prover. For example, the UWB-based designs [65, 136, 138] require the prover to be capable of receiving and transmitting UWB pulses. The CRCS design [118] requires the prover to be able to switch frequencies. Moreover, the absence of challenge interpretation during the rapid-bit exchange phase makes the system vulnerable to simple response replay attacks. In order to prevent such attacks, the prover needs to demodulate, store and communicate the challenges back to the verifier during the final verification phase of the protocol. This further increases the complexity of the prover making current implementations unsuitable for power-constrained applications such as contactless access control and authentication systems. In summary, today's solutions for secure proximity verification are not suitable for a number of applications; specifically that of contactless systems such as payment and access control systems. Additionally, the most efficient solutions are insecure against strong attackers. In the following chapters, we address the above-mentioned shortcomings and present our solutions.

Chapter 3

Switched Challenge Reflector with Carrier Switching

3.1 Introduction

In this chapter, we address the problem that existing analog-only distance bounding designs are only resilient against distance and mafia fraud attacks but not resilient against terrorist fraud attacks. Recall that, distance bounding protocols rely on the exchange of timed challenges and responses between the verifier and the prover. However, given that the prover is not trusted by the verifier and no assumptions can be made about its processing capabilities, the time that the prover spends in processing the verifier's challenge should be negligible compared to the measured round-trip time, which depends on the speed of light. If the verifier would overestimate the prover's processing time (i.e., the prover is able to process signals in a shorter time than expected), the prover would be able to pretend to be closer to the verifier. The challenge in implementing distance bounding protocols is therefore to implement a prover that is able to receive, process and transmit signals in negligible time.

Although a number of protocols have been proposed, it is not clear if the proposed distance bounding protocols can be implemented with the required tight processing (and therefore security) guarantees or can be integrated within the existing RF ranging systems. For example, almost all distance bounding protocols assume that a prover will be able to receive a single bit of the challenge, XOR it or compare it with some locally stored value, and transmit the response; all within negligible time. XORs and comparisons require digital processing and the most efficient implementation in the open literature that can realize such distance bounding protocols requires 100 ns [136, 138] and thus enables the attacker to cheat on its distance by at most 15 m. An alternative implementation of distance bounding protocols, using analog processing was proposed in [118] enabling signal reception/processing/transmission within 1 ns and thus provided a tight security guarantee of 15 cm. Instead of using XOR or comparison, this design relied on a processing function called Challenge Reflection with Channel Selection (CRCS), which can be implemented using only analog processing techniques. In [65], a design for implementing a secure distance bounding channel for the rapid bit-exchange in a near-field environment was presented. The experimental implementation used improvised wideband pulses and achieved a distance bound of 1 m in the case of mafia fraud attacks and 11 m for distance frauds.

However, even if implementing distance bounding using analog processing techniques clearly provide tighter security guarantees than digital implementations, existing analog implementations are not resilient against *terrorist fraud* attacks [24]; they are only suited for the prevention of *distance fraud* and *mafia fraud* attacks. In this chapter, we address this problem, and propose a new hybrid digital-analog design of a distance bounding system called *Switched Challenge Reflector with Carrier Switching* that enables the implementation of terrorist fraud resilient distance bounding protocols such as the Swiss Knife Protocol [82]. Our system does not introduce new processing functions at the prover (such as CRCS); instead, it uses the *bit comparison* function that is commonly used in a number of distance bounding protocols including the Hancke-Kuhn protocol [67].

In our proposed design, the verifier transmits challenges on two different carrier frequencies; the switching time synchronized with the prover. Four possible reply channels are created before activating the appropriate reflected carrier frequency. Based on the credentials held by the prover and the carrier frequency of the received challenge, an activation circuity inside the system appropriately enables the reply channel. Analysis of our prototype shows that the verifier can be cheated only up to 4.5 m in the scenario of a terrorist fraud attack and further only up to 0.41 m under a distance or mafia fraud attacker model. Given its design, our system can be used to implement existing terrorist fraud resilient distance bounding protocols (e.g., the Swiss Knife protocol [82]). Furthermore, it can be used to implement all distance bounding protocols that follow the Hancke-Kuhn construction [67] without requiring any modifications of the protocol.

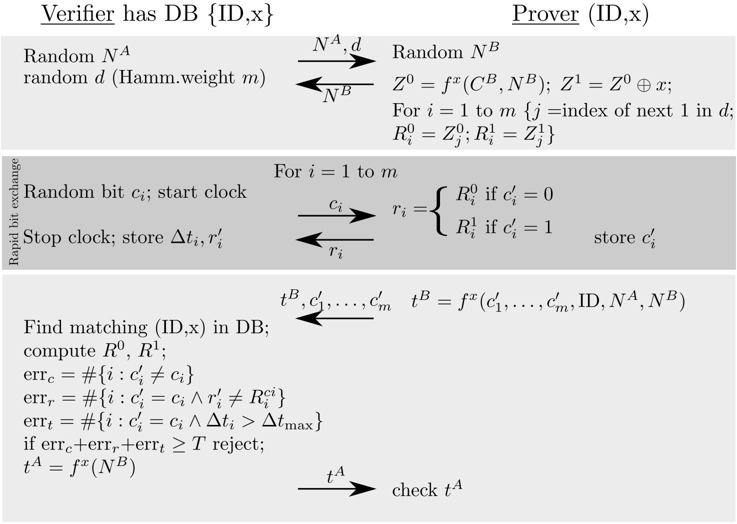

Verifier has DB {ID,x}
Prover (ID,x)
Random N^A
random d (Hamm.weight m)
N^A, d
N^B
Random N^B
$Z^0 = f^x(C^B, N^B)$; $Z^1 = Z^0 \oplus x$;
For $i = 1$ to m {j =index of next 1 in d;
$R_i^0 = Z_j^0; R_i^1 = Z_j^1$}
Rapid bit exchange
For $i = 1$ to m
Random bit c_i; start clock
c_i
$r_i = \begin{cases} R_i^0 \text{ if } c_i' = 0 \\ R_i^1 \text{ if } c_i' = 1 \end{cases}$
Stop clock; store $\Delta t_i, r_i'$
r_i
store c_i'
$t^B, c_1', \ldots, c_m'$
$t^B = f^x(c_1', \ldots, c_m', \mathrm{ID}, N^A, N^B)$
Find matching (ID,x) in DB;
compute R^0, R^1;
$\mathrm{err}_c = \#\{i : c_i' \neq c_i\}$
$\mathrm{err}_r = \#\{i : c_i' = c_i \wedge r_i' \neq R_i^{ci}\}$
$\mathrm{err}_t = \#\{i : c_i' = c_i \wedge \Delta t_i > \Delta t_{\max}\}$
if err_c+err_r+$\mathrm{err}_t \geq T$ reject;
$t^A = f^x(N^B)$
t^A
check t^A

Figure 3.1: *The Swiss Knife protocol. Picture adapted from [82].*

3.2 Terrorist Fraud Resilient Protocols

Terrorist fraud resilient protocols [55, 66, 82, 141, 143] preserve the basic structure of distance bounding protocols, but bind the prover's long-term secret to the nonces that are exchanged in the protocol. This prevents the prover from simply handing over the nonces to the external attacker without disclosing its long term secret.

We illustrate the operation of these protocols through an example: the *Swiss Knife* protocol. This protocol was proposed by Kim *et al.* [82] (Figure 3.1). The protocol assumes that the verifier has a database containing prover identities (ID) and their symmetric keys (x) and that each prover possesses his own identifier and key. The protocol is executed in three phases.

Preparation phase: From its locally generated nonce N^B, a shared secret x and a constant C^B, the prover creates two m-bit strings (R^0 and R^1) using a keyed pseudorandom function f. Disclosing both R^0 and R^1 would immediately reveal m bits of x.

Rapid-bit-exchange phase: In each round i of the rapid-bit-exchange phase, the verifier sends a random single-bit challenge c_i. Upon reception of c_i', the prover replies with the value taken from R_i^0, if $c_i' = 0$ and from R_i^1, if $c_i' = 1$. c_i'

denotes the modification of c_i over the channel either due to an attack or due to transmission errors.

Concluding phase: The prover sends a Message Authentication Code (MAC) computed over the nonces and the received challenges. The verifier then makes a number of checks: he tries to find an entry x in his database for which the MAC is valid; he checks if the number of transmission errors in the challenges are not too high; if the number of incorrect responses to correctly received challenges is not too high; and if the responses were sent in time. If all these checks pass, the verifier authenticates itself to the prover by computing a MAC on the prover's nonce N^B. In this protocol, the values of the registers R^0 and R^1 are bound to the prover's long term secret x. If the prover would like to perform a terrorist attack, it would need to give R^0 and R^1 to the external attacker, thus disclosing x.

As summarized in Chapter 2, so far, in the space of distance bounding protocol implementations, we could either build efficient implementations, that resist distance fraud and mafia fraud but not terrorist fraud attacks, or less efficient implementations that resist all three types of attacks.

3.3 Switched Challenge Reflector with Carrier Shifting

As discussed in Section 3.2, one of the open problems in distance bounding protocol design space is the realization of terrorist fraud resilient distance bounding with low processing delay at the prover. Prover designs based on digital signal processing techniques allow implementation of processing functions such as XOR or register read-out based on the challenge bits. However, the process of demodulating the received challenge, computing the response (e.g., XOR with a shared secret), modulating and transmitting back the response incurs significant processing delay [118]. This delay allows attackers executing distance and mafia frauds to gain distance in the order of several tens of meters. Although solutions using only analog processing techniques achieved low processing delay, implementing processing functions such as register selections (critical for terrorist fraud resilience) give rise to new attack scenarios. Due to the nature of analog signals and components, such solutions based on register selection are vulnerable to a new attack that we refer to as the *double read-out* attack (detailed in Section 3.4) which could potentially leak the long-term shared secret. Here we present a hybrid digital-analog solution to this problem, which we refer to as *Switched Challenge Reflector with Carrier Shifting (SCRCS)*. We show that a prover implementing SCRCS

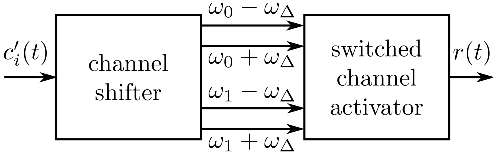

$c_i'(t)$
channel shifter
$\omega_0 - \omega_\Delta$
$\omega_0 + \omega_\Delta$
$\omega_1 - \omega_\Delta$
$\omega_1 + \omega_\Delta$
switched channel activator
$r(t)$

Figure 3.2: *Overview of the switched challenge reflector with carrier shifting.*

has low processing delay and resists not only mafia and distance frauds but also terrorist fraud attacks without allowing any possible double read-out attacks.

3.3.1 Design Overview

In terrorist fraud resilient protocols [82, 120, 141], the verifier challenges the prover with randomly selected bits; in each of the m rounds, based on the received challenge bit the prover replies with a bit from one of the two local registers. The prover's processing, therefore, consists of receiving the challenge bit and then transmitting a bit from one of the registers, selected based on the received challenge bit. We design SCRCS to implement this functionality.

In our system, the verifier challenges the prover with a challenge signal $c(t)$; if the verifier wants the prover to respond with a value from register R^0, it transmits a signal on a predefined carrier frequency ω_0 (encoding the challenge bit "0") and if it wants to query R^1, it transmits on the carrier frequency ω_1 (thus encoding the challenge bit "1").

The prover implements switched challenge reflection with carrier shifting. Figure 3.2 shows the two main building blocks of the prover: (i) Channel Shifter and (ii) Switched Channel Activator. The prover takes as input the challenge signal $c(t)$, which will be at the carrier frequency ω_0 or ω_1; its Channel Shifter component (details in Section 3.3.2) creates two copies of the received signal: at $\omega_0 + \omega_\Delta$ and $\omega_0 - \omega_\Delta$ or at $\omega_1 + \omega_\Delta$ and $\omega_1 - \omega_\Delta$ where $\omega_\Delta < (\omega_1 - \omega_0)/2$. The two created signals (e.g., the signals at $\omega_0 \pm \omega_\Delta$) are then fed into the Switched Channel Activator circuit which then, depending on the current value of the queried register, outputs ($r(t)$) only one of the two signals (e.g., the signal at $\omega_0 + \omega_\Delta$). The Switched Channel Activator circuit is constructed such that it only allows either the signals at $\omega_0 \pm \omega_\Delta$ or signals at $\omega_1 \pm \omega_\Delta$ but not both simultaneously.

The start of each rapid bit exchange round i.e., the times at which the verifier switches its challenge carrier frequency is synchronized with the prover. This is achieved by the verifier sending an initial preamble defining the exact starting time of the rounds in the rapid-bit exchange phase. This allows

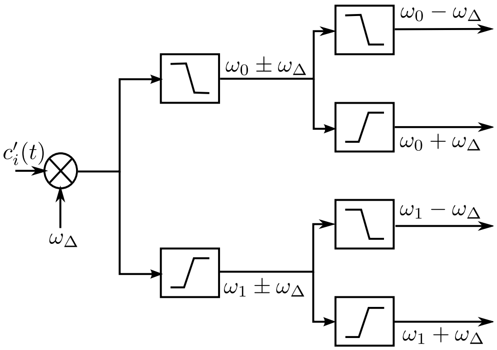

$c'_i(t)$
ω_Δ
$\omega_0 \pm \omega_\Delta$
$\omega_1 \pm \omega_\Delta$
$\omega_0 - \omega_\Delta$
$\omega_0 + \omega_\Delta$
$\omega_1 - \omega_\Delta$
$\omega_1 + \omega_\Delta$

Figure 3.3: *The channel shifter. The incoming signal $c(t)$ contains the challenges on either carrier frequency ω_0 or ω_1. After mixing $c(t)$ with ω_Δ, the signal is filtered appropriately to generate the four possible response channels: $\omega_0 - \omega_\Delta, \omega_0 + \omega_\Delta, \omega_1 - \omega_\Delta, \omega_1 + \omega_\Delta$.*

the prover to provide an accurate clock to the switched channel activator block (details in Section 3.3.3) that is responsible for enabling the appropriate reply channel.

3.3.2 Channel Shifter

The channel shifter receives the incoming challenge signal $c'(t)$ and applies filters creating four possible reply channels. Figure 3.3 illustrates in detail the operation of channel shifter module. The received challenges are mixed with an offset frequency ω_Δ ($\omega_\Delta < (\omega_1 - \omega_0)/2$). Based on the carrier frequency on which the challenge is transmitted, the mixer output signal consists of two out of four possible frequency components ($\omega_0 \pm \omega_\Delta$ or $\omega_1 \pm \omega_\Delta$). A set of low-pass and high-pass filters separate the frequency components resulting in four possible reply channels. These are then fed into the switched channel activator block.

3.3.3 Switched Channel Activator

The switched channel activator module enables the appropriate reply channel based on the amount of energy detected in each of the four signals output by the channel shifter. The module consists of two clocked registers R^0 and R^1, a channel activation circuitry and a memory element to store which channel was activated every round as shown in Figure 3.4. Both the memory and registers R^0 and R^1 are clocked with the signal CLK, which signals the start of

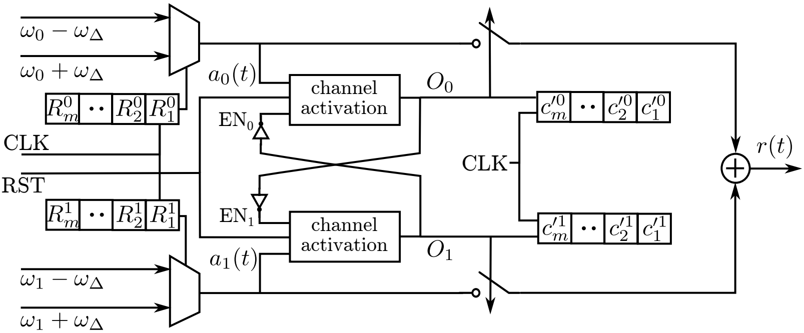

$\omega_0 - \omega_\Delta$
$\omega_0 + \omega_\Delta$
R^0_m ·· R^0_2 R^0_1
CLK
RST
R^1_m ·· R^1_2 R^1_1
$\omega_1 - \omega_\Delta$
$\omega_1 + \omega_\Delta$
$a_0(t)$
EN$_0$
EN$_1$
$a_1(t)$
channel activation
channel activation
O_0
O_1
CLK
c'^0_m ·· c'^0_2 c'^0_1
c'^1_m ·· c'^1_2 c'^1_1
$r(t)$

Figure 3.4: *Switched channel activator. The registers R^0 and R^1 select which two of the four reply channels are used in this round. The channel in which sufficient energy is encountered first gets enabled. After a channel is activated, it stays active until the end of this rapid bit-exchange round while the other channels remain de-activated until the end of this round.*

each round in the rapid bit-exchange phase of the protocol. The output $r(t)$ depends on the carrier frequency of $c'(t)$ and the content of R^0 and R^1 during the current round. For example, if the challenge is sent on ω_i, the output is on the channel $\omega_i + (2R^i - 1)\omega_\Delta$. The channel activation circuitry detects the carrier frequency of the challenge signal based on energy detection. Once a channel is activated, it will disable the other channel's activation circuit (i.e. $O_1 = \overline{EN_0}$).

Channel Activation: Figure 3.5 shows the internals of the channel activation circuitry. The channel activation mechanism ensures that only one of the output channels is activated in each round of the rapid-bit exchange. After this initial activation, the channel then stays active for the remainder of the current round, reflecting all challenges on this frequency. This selection requires an initial energy and carrier detection, which takes δ_a time in each round of the rapid bit exchange. After δ_a, the correct reply channel is activated and reflects $c'(t)$ with very low delay (incurred by mixing and filtering). The selection of the reply channel is based on the first carrier frequency which contained energy above the threshold T^E. After each round in the rapid bit exchange, all reply channels are deactivated by asserting the RST signal until energy is encountered again in the next round.

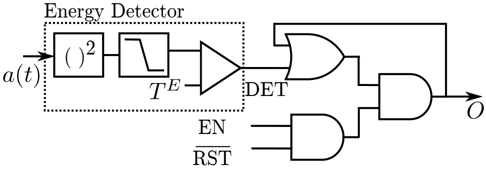


Figure 3.5: *Internals of channel activation. We obtain a DC component of the squared signal to detect energy in the channel and store the value for this round in a latch-like circuit. The channel activation can be disabled by pulling EN (enable signal) low and is automatically reset at the beginning of each round of the rapid-bit exchange (RST).*

Security of terrorist fraud resilient protocols relies on the fact that extracting the contents of both the registers R^0 and R^1 compromises the long-term shared secret. In a fully digital implementation of provers, it is not possible to read-out both the register contents simultaneously. However, in our design due to the nature of analog signals and components, there is a possibility of extracting both register contents. We explain this in detail in Section 3.4. The important role of the channel activation module is to prevent an attacker from executing such *double read-out* attacks by ensuring only one reply channel is active at any given point in time of a particular round.

Synchronization between the verifier and prover: Synchronization between the verifier and the prover is essential for easy verification of the reflected signal later in the concluding phase of the protocol. As discussed in Section 3.3.1, a preamble sequence transmitted by the verifier is used to establish this synchronization and to generate the switched channel activator's CLK signal. Using this clock, channels are reset at the start of each round of the rapid bit-exchange. It is important to note that the processing time of the preamble does not have strict limitations or security implications. The prover can take some deterministic time δ_p to process the preamble, as long as the challenge data sequence starts at a time greater than δ_p after the preamble.

3.4 Security Analysis

We investigate the security impact of our proposed distance bounding system with respect to each of the three attack scenarios. In addition, we consider a fourth attack: *double read-out attacks* on terrorist and mafia fraud resilient systems with multiple registers at the prover side.

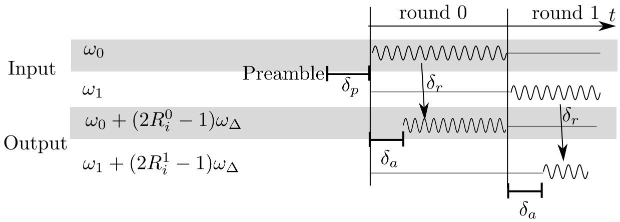


Figure 3.6: *Timing related variables for challenge reflection. In each round, channel activation adds an initial delay δ_a. After channel activation, the challenges are reflected with a very small delay δ_r. The start time of each round depends on the initial preamble synchronization by the prover.*

3.4.1 Resilience Against Distance Fraud Attacks

In distance fraud attacks, the malicious prover is further than D away from the verifier. In order to shorten the measured distance, he will have to send the reply signal $r(t)$ earlier than an honest prover. To achieve this goal, the prover has two options: (a) predict the challenge signal $c(t)$, including the carrier frequency used for each round, or (b) reflect $c(t)$ in with less delay than expected.

The probability to correctly predict the challenge signal $c(t)$ for m rounds of rapid bit exchange depends on the nature of the baseband data signal modulated on the challenge carrier. In the worst case, a constant data signal is modulated on the carrier, which enables the malicious prover to predict it. In this case, our system matches the security analysis of the distance bounding protocol it is used in, as the malicious prover only has to predict which of the registers R^0 and R^1 gets queried in each round. If the baseband signal in $c(t)$ contains data which is unpredictable for the prover, the chance to send an early correct $r(t)$ is strictly smaller than predicted by the overlying protocol. An exact specification depends on the nature of the baseband data signal.

In the following, we analyze the security impact of timing parameters (see Figure 3.6).

Reflection delay (δ_r): Even if the malicious prover can reflect the challenge with less delay than expected, this will only yield an improvement in the order of nanoseconds. In our implementation, the reflection delay δ_r once the channel is activated is around 3 ns. This means the attacker can only gain a distance advantage of 50 cm by reducing δ_r to 0.

Activation delay (δ_a): If the prover is able to shorten δ_a, the correct channel can be activated sooner. Nevertheless, this will not shorten the reflection delay δ_r, and therefore not influence the measured distance for this attack case.

Round start time (δ_p): In our design, we assume that the prover was able to establish the exact start time for each round due to a synchronization preamble sent earlier. This time is required to successfully run the protocol—if the timing is changed, the protocol will most likely fail, instead of returning a wrong distance measure.

If the malicious prover (or external attacker) advances the local round start time of the prover, the channel might be activated by the previous round's carrier frequency. This leads to incorrect reflection of the challenge in 50% of the rounds. If the round start time at the prover is delayed, the prover will not switch to the correct reply channel early enough. Since we have a strict requirement for δ_a, the channel activation delay, this will also cause the protocol to fail. Therefore, changing the round start time does not give an advantage to either malicious prover or external attacker.

3.4.2 Resilience Against Mafia Fraud Attacks

In the mafia fraud, an external attacker close to the verifier tries to impersonate the prover. To successfully impersonate the prover, the attacker can either (a) guess the content of the registers R^0 and R^1 in advance (with probability as predicted in the original protocols), or (b) try to send *early challenges* to the honest prover, to obtain the actual content of registers in advance. Since our system allows the prover to record the received challenges, these can be sent to the verifier in the concluding phase of the protocol later. If the protocol performs this reconciliation on the received challenges, the attacker will have to correctly predict the challenge carrier frequencies used in each round of the rapid-bit-exchange to avoid detection. If no reconciliation phase is supported by the protocol (as in [67]), the attacker's chances are better as discussed in the original protocol.

As the mafia fraud is an external attack, the attacker cannot influence the processing delays δ_p, δ_a and δ_r of an involved honest prover. The same reasoning as in the distance fraud attack holds good for the round start time. Any modification to the round start time will only result in failure of the protocol execution.

3.4.3 Resilience Against Terrorist Fraud Attacks

In a terrorist fraud attack, an attacker close to the verifier tries to impersonate the prover. The prover will support the attacker if it does not compromise his long-term secret. In our rapid-bit-exchange scheme, the content of both registers R^0 and R^1 is needed by the attacker to successfully impersonate the prover. But as both register values combined allow the attacker to derive the long-term secret, the prover will not be able to provide these.

Another possibility is for the attacker to early detect the current round's challenge carrier frequency, forward it to the malicious prover and obtain that round's register value. In this case, the long-term secret of the malicious prover would not be revealed. To estimate the impact of this attack, we consider a strong attacker and prover with both zero processing time for incoming challenges and messages. In this setting, the attacker could use the channel activation time at the start of each round to forward the current round's challenge carrier frequency. In this setting, the attacker could shorten the measured distance by up to $\delta_a/2$. As this delay is typically short ($< 30\,\text{ns}$ in our implementation), the maximal gain is only in the range of few meters ($\approx 2.5\,\text{m}$ for $30\,\text{ns}$ and instantaneous processing).

Reducing the preamble processing delay δ_p will not yield an advantage to the attacker, while a reduction of the reflection delay can reduce the measured distance as discussed above.

3.4.4 Double Read-out Attacks

The double read-out attack targets a potential implementation weakness of analog provers with multiple registers. If the attacker manages to simultaneously query (read-out) the values from both registers of the prover, he would be able to reconstruct the prover's long-term secret in terrorist fraud resilient protocols. In the case of mafia fraud resilient protocols, this would allow the attacker to mount a mafia fraud attack instead.

Analog implementations e.g., those that would build on CRCS [118] would typically allow a double read-out attack, since they would not prevent the verifier (and the attacker) to transmit the challenge signals on both carrier frequencies simultaneously. To prevent this attack, a digital component is needed (e.g., a channel activation component) that prevents that both register values are transmitted by the prover simultaneously.

More precisely, consider our SCRCS scheme without the channel activation part, i.e. we assume that only the challenge signal and the values of R^0 or R^1 are used to determine the reply channel. In this setting, the attacker could craft a challenge signal which alternates between two challenge carrier frequencies within each round of the rapid bit-exchange and obtain the content of both registers, allowing him to derive the prover's long term secret. Although this attack will most likely be detected by challenge reconciliation in the concluding phase (the MAC'ed c' sent by the prover), the long term secret would still be revealed to the attacker.

In our system, this attack is prevented by the channel activation circuit—this circuit will only allow one register to be read in each round (see Figure 3.4 and Figure 3.5). To show that both registers can never be read at the same round, we first show that signal O_i, once activated, can only be deactivated by $\overline{\text{RST}}$. In Boolean logic, we can write $O_i = (\text{DET}_i \vee O_i) \wedge \overline{\text{RST}} \wedge \text{EN}_i$, with $\vee$ as boolean OR and $\wedge$ as AND. Therefore, once O_i is high, it only transitions to false (low) if either $\overline{\text{RST}}$ or EN_i are low. Using $j = |i - 1|$ we can write $\neg\text{EN}_i = O_j$. Therefore, once O_i is true (high) and assuming that $\overline{\text{RST}}$ is high, O_i can only turn false if O_j is also true. Using the equation above, one can write $\text{EN}_i = \neg[(\text{DET}_j \vee O_j) \wedge \overline{\text{RST}} \wedge \text{EN}_j]$. Since O_i is true and $\text{EN}_j = \neg O_i$, O_j will always return false. Summarizing, this result shows that a channel can only be deactivated if both channels are true, which cannot happen once one channel is activated. Therefore, both registers cannot be read in the same round.

In addition, our design also prevents unintentional double read-out by the verifier, which might occur if the round start timing of the prover is not aligned well with the verifier. As discussed above, our channel activation will cause the protocol to fail in this case, instead of unintentionally revealing the long-term secret of the prover.

3.5 Implementation and Analysis

In this section, we describe our prototype implementation of the prover and the results of our experiments. We implement our design using commercially available RF modules [7]. The analog components of the prover implementing the switched challenge reflection with carrier shifting is shown in Figure 3.7. The two carrier frequencies $\omega_0 = 3.5\,\text{GHz}$ and $\omega_1 = 5\,\text{GHz}$ used for transmitting the challenge signal $c(t)$ are generated using function generators and given as input to the prover.

3.5.1 Channel Shifter

As described in Section 3.3.2 the channel shifter is implemented using a mixer and six filters (3 low-pass and 3 high-pass). In Figure 3.7, components 1–4d constitute the channel shifter module. The received signal is amplified and

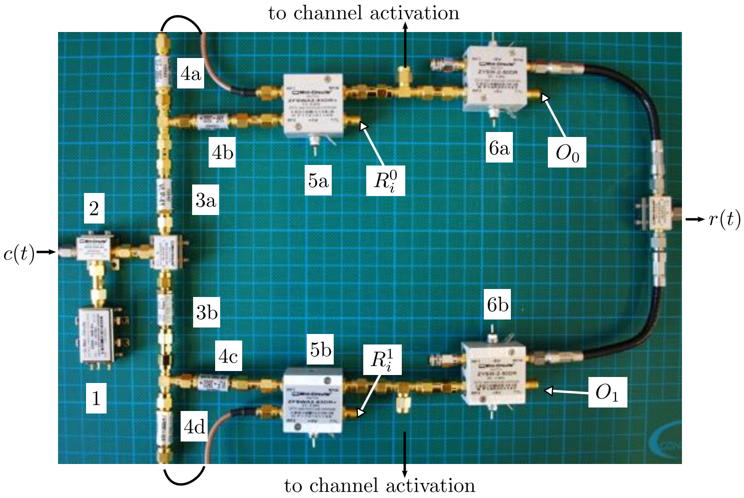


Figure 3.7: *Experimental Setup: 1: voltage controlled oscillator; 2: mixer; 3a,3b, 4a, 4b, 4c, 4d: filters that constitutes the channel shifter module; 5a, 5b: switches whose output depends on the contents of registers R_i^0 and R_i^1; 6a, 6b: switches that activate the reply channel based on the channel activation circuit outputs (O_0, O_1).*

mixed (2) with an intermediate frequency $\omega_\Delta = 500\,\text{MHz}$ generated by a voltage controlled oscillator (1).

Depending on the received carrier frequency (ω_0 or ω_1), the mixer output contains either the frequency components $\omega_0 \pm \omega_\Delta$ or $\omega_1 \pm \omega_\Delta$. This signal now passes through the combination of low-pass and high-pass filters separating the signal into four possible reply channels. For example, if $c(t)$ was transmitted on ω_0, the filters 3a, 4a and 4b (see Figure 3.7) create the signals with frequency components $\omega_0 + \omega_\Delta$ and $\omega_0 - \omega_\Delta$. Similarly for ω_1, filters 3b, 4c and 4d output $\omega_1 + \omega_\Delta$ and $\omega_1 - \omega_\Delta$. These shifted signals are then fed to the switched channel activator block.

3.5.2 Channel Activation

The channel activation circuitry constitutes an important part of the prover design to prevent double read-out attacks, as explained in Section 3.4. The circuit is implemented using a mixer squaring the signal followed by a low-pass filter and a switch. The output of the low-pass filter is the control voltage for the switch. The switch, with one input connected to 5V and the other

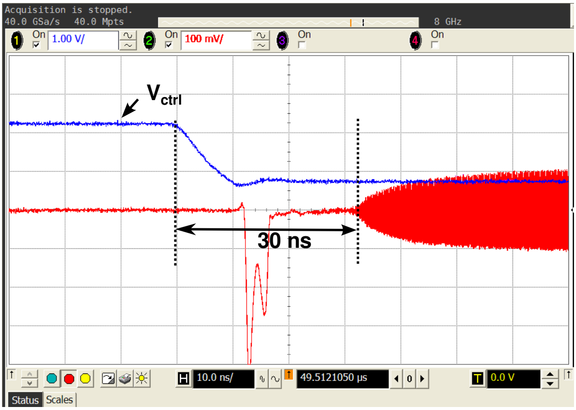

Acquisition is stopped.
40.0 GSa/s 40.0 Mpts
8 GHz
1 On 1.00 V/
2 On 100 mV/
3 On
4 On
H 10.0 ns/
49.5121050 µs
T 0.0 V

Figure 3.8: *Delay in switching channels.*

grounded acts as a threshold detector whose output is a logic high when its control voltage is above T^E.

We measured the time delay of the channel activation circuitry from the moment the signal is available for energy detection (output of switches 5a, 5b) until the channel is actually activated or deactivated (depends on control signals O_0, O_1 to switches 6a, 6b). Figure 3.8 shows the control voltage V_{ctrl} and the channel signal. We can see that the switching delay δ_a is approximately 30 ns. As discussed in Section 3.4 the delay δ_a does not have any security implications in the scenarios of distance and mafia frauds. In the case of terrorist fraud an attacker can shorten the distance only up to 4.5 m for $\delta_a =$ 30 ns.

3.5.3 Challenge Reflection Delay

The time taken by the prover to process and reflect back the challenge (δ_r) directly impacts the maximum distance advantage an attacker gains as discussed in Section 3.4. The challenge signal $c(t)$ is pulse modulated using a 2 μs pulse in order to capture and estimate the delay more accurately. The challenge is processed by the prover circuit, and the delay is estimated by tapping into the signal at the circuit's input and output. An oscilloscope with high sampling rate of 40 GSa/s is used to visualize the delay of the signals. Figure 3.9 shows both input challenge signal and the prover output with a delay of approximately 2.75 ns. This implies that a dishonest prover can gain a maximum distance of 0.41 m by implementing SCRCS with 0 ns delay. The

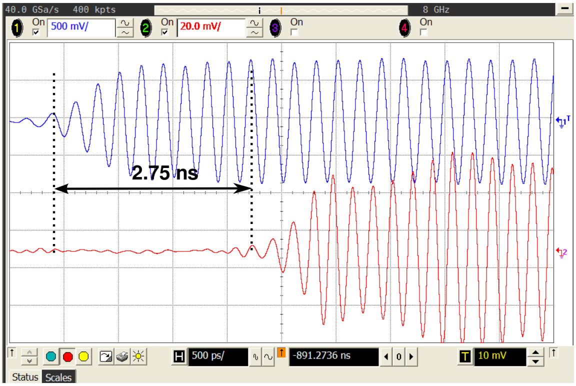


Figure 3.9: *Prover path delay: The total delay incurred due to mixing, filtering and channel activation switch is estimated to be 2.75ns.*

measured delay is independent of the carrier frequency on which the challenge is transmitted and same for both the carrier frequencies (ω_0 and ω_1).

Table 3.1 summarizes all the delays and the attack scenarios in which they are applicable. It is important to note that these delays would be further reduced by implementing the system as an integrated circuit.

Delay	Max. distance gained	Attack Scenario
$\delta_r = 2.75\,\text{ns}$	0.41 m	DF, MF and TF
$\delta_a = 30\,\text{ns}$	4.5 m	TF
δ_p	-NA-	-NA-

Table 3.1: *Summary of prover delays and the attack scenarios under which they are applicable. Reducing or enlarging round start time δ_p would only cause the protocol to fail.*

3.6 Conclusions

In this chapter, we designed and implemented a distance bounding system that is resilient to the three well-known distance modification attacks: Distance, mafia and terrorist frauds. Our mixed digital-analog realization allows challenge processing delays of the order of few nanoseconds, thereby limiting the maximum distance an attacker can cheat on. To the best of our knowledge, this is the first implementation of a distance bounding system that is secure against all the three forms of attacks, while having a low processing delay. We introduced a new attack called the “double read-out” attack and showed how our proposed system is secure against it.

With the example of the Swiss Knife protocol, we illustrated how our system design allows implementation of existing terrorist fraud resilient protocols and also other distance bounding protocols that are based on the Hancke-Kuhn construction model. We conclude from the delay measurements of our prover prototype that the attacker will be able to decrease distance by not more than 4.5 m in the terrorist fraud scenario. This was derived from the processing delay of 2.75 ns and delay incurred during channel activation. This bound further reduced to 0.41 m for the distance and mafia fraud cases.

System Limitations: Even though the design proposed above is resilient to all the three well-known distance bounding attacks, the design requirements are still complex for use in power-constrained applications such as contactless systems. For example, like CRCS [118], SCRCS [115] also require the prover to receive and transmit using multiple frequencies. This leads to an increased overall system bandwidth. Furthermore, implementing SCRCS requires a number of high-pass and low-pass frequency filters, signal mixers, and intermediate frequency generators at the prover which makes it difficult to integrate with many access control and authentication applications in which the prover (e.g., contactless card) is required to be fully passive. We address this problem in Chapter 5 of this thesis.

Chapter 4

Security Analysis of Chirp-based Ranging Systems

4.1 Introduction

Today, for short and medium-distance precision ranging and localization, ultra wideband (UWB) and chirp spread spectrum (CSS) emerged as the most prominent techniques and were standardized in IEEE 802.15.4a [77] and ISO/IEC 24730-5 [78]. Their ranging resolution and reliability makes them suitable for numerous applications including indoor asset tracking and guidance [123], loss protection [14], etc. While UWB provides robust and precise distance measurements, the difficulties of building small size, low-power receivers has currently limited its use. However, the properties of CSS [26, 133] allow low-complexity and low-power implementations of both the transmitter and receiver on a single integrated hardware [102]. This enables the realization of two-way distance-ranging solutions using RTOF with relatively high distance resolution (1 m) [14].

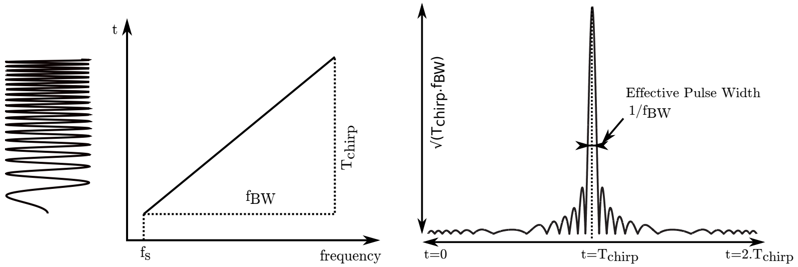
In this chapter, we analyze the security of CSS-based ranging systems. Although CSS-based ranging solutions have already been commercialized (e.g., for child-monitoring, mine safety, warehouse monitoring systems), their security, and therefore their suitability for security- and safety-critical applications have so far not been evaluated. The implications of distance modification attacks in scenarios where these systems are deployed in security-critical applications like access control to automobiles, buildings and medical devices are significant. Recent examples of attacks on the physical distance (e.g., on near-field communication (NFC) payment systems [58], passive vehicle keyless entry systems [57]) further motivate the need for investigating and understanding the security implications of physical-layer distance measurement mechanisms. Such understanding enables us to evaluate their use in security-critical applications.

The contributions of this work are as follows. We analyze the security of CSS-based ranging systems, focusing on standardized schemes adopted in the ISO/IEC 24730-5 standard for real-time localization (RTLS) and used in a commercial-of-the-shelf (COTS) ranging system [103]. We show that distance modification attacks on CSS-based ranging systems are feasible by exploiting the inherent physical properties of chirp signals; we focus on attacks which result in a decrease of the measured distance since these have been shown to be most relevant in the majority of security applications. We validate our findings by simulations and measurements from COTS CSS transceivers in several indoor locations to account for real-world channels. Our distance decreasing attacks account for the attacker's hardware delays and thus are close to practical conditions. Our results demonstrate that an attacker would be able to effectively reduce the distance estimated by a trusted distance-ranging system by more than 150 m for typical short chirp durations and more than 700 m for longer chirps. Since the attacks exploit physical-layer characteristics of CSS communication, we show that higher-layer cryptographic mechanisms cannot prevent these attacks. Finally, we discuss possible countermeasures against these attacks.

The remainder of this chapter is organized as follows. In Section 4.2, we provide a brief overview of CSS-based ranging systems. In Section 4.3, we define and discuss the attacks that can be mounted on chirp-based ranging systems. In Section 4.4, we describe our experimental setup and evaluate the feasibility of the proposed attacks through simulations and experiments. We also discuss the implication of our findings. In Section 4.5, we enumerate possible countermeasures. We provide the related work in Section 4.6 and conclude the chapter in Section 4.7.

4.2 Background: Chirp Spread Spectrum

In this section, we provide an overview of chirp signals and the pulse compression technique commonly used by radar systems for distance measurement. We then describe the architecture of typical chirp-based ranging systems and



(a) *Frequency vs Time representation of chirp signal.*

(b) *Result of pulse compression.*

Figure 4.1: *Chirp signals: (a) The linear variation of chirp signal frequency with time. (b) Compressed pulse output of the matched filter.*

discuss the existing CSS standards and commercially available chirp-based ranging solutions.

4.2.1 Chirp Signals

Chirps are sinusoidal signals whose frequency varies with time. Depending on the type of chirp, the frequency variation is linear or exponential. Chirp signals [26] have been extensively used in radar and sonar systems [40, 107] to determine, among other characteristics, range, velocity, and angular position of a target object. The representation of a linear chirp signal $y(t)$ is shown in Equation 4.1, where f_s is the starting sweep frequency and α represents the rate of change of frequency (sweep rate) of the chirp signal. Figure 4.1a shows how the chirp signal changes in frequency with time. Equation 4.2 gives the sweep rate α of the signal in terms of the chirp duration T_{chirp} and chirp bandwidth ω_{BW}.

$$y(t) = sin[2\pi(f_s + \alpha \cdot t)t] \tag{4.1}$$

$$\alpha = \frac{\omega_{BW}}{2 \cdot T_{chirp}} \tag{4.2}$$

$$f(t) = f_s + \alpha \cdot t \tag{4.3}$$

Due to the linear frequency sweep, chirp signals can be efficiently compressed to pulses referred to as *pulse compression*. This is achieved by correlating the received chirp signal with its matched filter. The output of the matched filter for a chirp signal input is a short pulse as shown in Figure 4.1b. The pulse width of the chirp T_{chirp} is compressed to an effective width of $1/\omega_{BW}$.

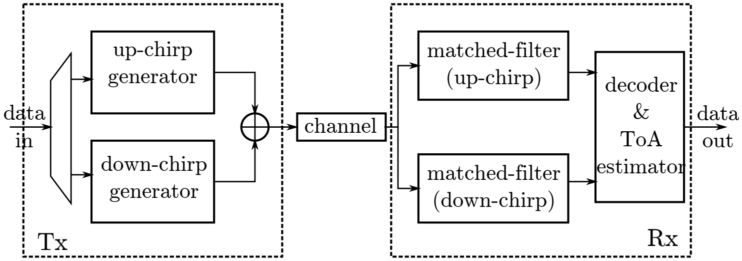


Figure 4.2: *Building blocks of a CSS system: Data is modulated using BOK scheme at the transmitter. The receiver decodes and estimates the time-of-arrival based on the matched filter outputs.*

The effective output of the matched filter is the combined energy of the chirp pulse over its entire duration. This results in a processing gain that increases the signal-to-noise ratio at the receiver, thus reducing the bit error rate. Chirp pulse compression combines high processing gain with the improved distance resolution of short pulses.

The use of chirp signals for communication provides several advantages. Chirp signals exhibit high effective bandwidth as they sweep through the entire frequency space. Due to the larger bandwidth, they are less susceptible to multipath and other channel disturbances. Another advantage is that chirps can be processed only using analog signal processing blocks e.g., SAW filters [132]. This allows low-complexity and low-power realization of both communication and ranging. The strong auto-correlation properties of the chirp signals add more robustness to distance measurements in multipath environments.

4.2.2 Chirp-based Ranging System

In this section, we describe the modulation and demodulation blocks of a generic chirp-based ranging system. We further explain how the time-of-arrival (TOA) of chirp signals is estimated to provide ranging information.

Data modulation and demodulation: There are typically two ways of modulating data in a chirp-based communication system: Binary Orthogonal Keying (BOK) and Chirp Direct Modulation (CDM). In the BOK scheme [153], ‘1’ is represented by a chirp with increasing frequency sweep and ‘0’ is represented by a decreasing frequency sweep. Monotonically increasing frequency sweep signals are referred to as “up-chirps” and decreasing frequency sweeps – “down-chirps”. Since the up- and down-chirps are mutually orthogonal, their cross-correlation is zero. This simplifies the receiver's decision making about which data bit is being transmitted. In the CDM scheme [61, 69], the data bits are modulated using a conventional modulation technique, such as *m-ary PSK*. The data is first modulated and then spread with a pre-configured chirp signal. Here, the chirps are primarily used for spreading and are independent of the underlying modulation technique. We focus the remainder of this paper on the *BOK* modulation scheme. Figure 4.2 illustrates the key blocks of a CSS-based communication system using BOK modulation. At the receiver, the signal is processed through two matched filters for up- and down-chirps respectively. The decision-making block compares the outputs of the matched filters to decode the data bit. It should be noted that for the extraction of ranging information, additional signal processing is required.

TOA estimation and ranging: Ranging with CSS-based systems relies on time-of-flight (TOF) measurements obtained by accurate time-of-arrival (TOA) estimation. There are two possible approaches to obtain the TOA of the chirp signal at the receiver. One uses dispersive delay lines to perform pulse compression. Different frequency components in a signal experience different delays in the delay line which results in a compressed pulse containing the summed energy of the entire chirp signal. The maximum peak of the delay line time response indicates the time of arrival. The TOA precision depends on the sampling rate of the time response. This approach distinguishes itself by low-power consumption as the dispersive delay lines are passive analog components.

A second approach consists of generating the compressed pulse by cross-correlating the received signal with a template chirp signal using a digital signal processor (DSP). The incoming chirp signals are sampled and fed to the DSP. The DSP correlator's output is also a compressed pulse as in the previous approach. The peak output indicates the signal TOA. This design would typically consume more power, but offers high flexibility as most of the signal processing is done in the digital domain.

Further processing techniques such as spectral estimation and sample interpolation could be used to increase TOA estimate precision. It should be noted that TOF measurements also depend on tight clock synchronization between the transmitter and receiver. Given that local clocks may not exhibit sufficient long-term stability, ranging systems work by round-trip time-of-flight measurements. In such case, the distance between two nodes A and B is given by $d = \frac{c.(t_{RTOF} - t_p)}{2}$, where c is the speed of light ($3 \cdot 10^8\,\mathrm{m/s}$), t_{RTOF} is the round-trip time elapsed and t_p is the processing delay at B before

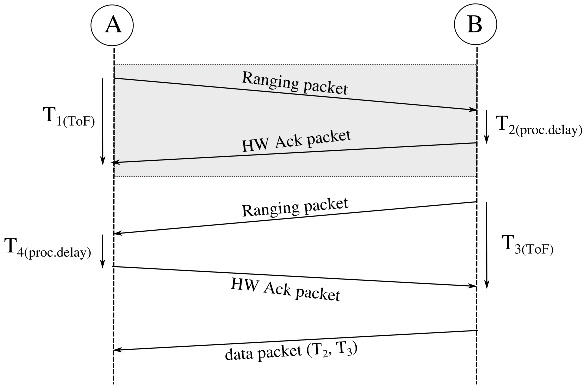


Figure 4.3: *SDS-TWR ranging scheme: RTOF measurements ($T_{1(ToF)}, T_{3(ToF)}$) are calculated by both nodes A and B. In the final step node B exchanges its time measurements with A. In a single-sided two-way ranging (highlighted), the RTOF measurement is calculated by node A only.*

responding to the ranging signal. This type of asynchronous ranging also often referred to as two-way time-of-flight ranging and does not require tight clock synchronization.

4.2.3 CSS Ranging Standards

In 2007, the IEEE 802.15.4a-2007 [77] standard was introduced to standardize lower network layers of wireless personal area networks with a strong focus on low-cost and low-rate communication between devices. This standard includes two physical-layer (PHY) specifications: ultra wideband impulse radio (UWB-IR) and chirp spread spectrum (CSS). ISO/IEC 24730-5:2010 [78] standardizes the use of CSS for ranging systems by defining air interface protocols and an application programming interface (API) for real-time localization systems (RTLS). The defined ranging protocol uses chirp spread spectrum at frequencies from 2.4 GHz to 2.483 GHz. It supports two-way TOF ranging and bidirectional communication between readers and tags of the RTLS.

Nanotron's Ranging Hardware: The NanoLOC transceiver from Nanotron is the only low-cost, low-power CSS-based ranging chip available off the shelf today. It uses BOK modulation and operates in the 2.4 GHz ISM band. Two nominal signal bandwidths are available on the chip: 22 MHz and 80 MHz.

The chirp duration is configurable with $T_{chirp} = 1.0, 2.0$ or $4.0\mu s$. The distance between two nodes is estimated based on the round-trip time-of-flight measurements. Since each module's local clock drifts introduces inaccuracies in the measurements, NanoLOC system executes a symmetric two-way ranging process referred to as *Symmetric Double-Sided Two-Way Ranging [SDS-TWR]*. The steps involved in the SDS-TWR scheme are illustrated in Figure 4.3. The first ranging measurement is calculated based on the RTOF from node A to node B and back to node A. A second measurement is determined with B initiating the ranging. In the final step node B shares the measured time values with node A. Node A computes its range estimate and the result is then averaged. This double-sided ranging mechanism mitigates the ranging inaccuracies due to local clock drifts at the nodes.

4.3 Physical-layer Attacks on CSS Ranging Systems

In this section, we investigate physical-layer distance decreasing attacks on CSS-based ranging systems. We state the system assumptions and discuss two distance decreasing attacks: by the early detection and by the late commit of chirp signals.

4.3.1 Early Detection and Late Commit Attacks

We consider two devices A and B that are able to communicate over a wireless radio link. The devices use the CSS BOK scheme for communication and ranging. We assume device A measures and verifies the distance claimed by device B. Device A is trusted and assumed to be honest. In this setting distance decreasing attacks can be mounted in two ways: (i) by a dishonest device B trying to cheat on its distance to A, referred to as an *internal attack* and (ii) by an external attacker who tries to shorten the distance between A and an honest device B, referred to as a *distance-decreasing relay attack*.

There are several ways for a dishonest device B to mount an internal attack. For example, device B can cheat on the distance by simply reporting incorrect values of T_2 and T_3 in the two-way ranging scheme as shown in Figure 4.3. Furthermore, device B can reduce its message processing time, thereby reducing the measured round-trip distance. The presented techniques in the remainder of this chapter can be used by a dishonest device B to decrease its distance to A without any loss of generality. We note that internal attacks can only be prevented by distance bounding techniques which enable very small and fixed processing delays [118, 137].

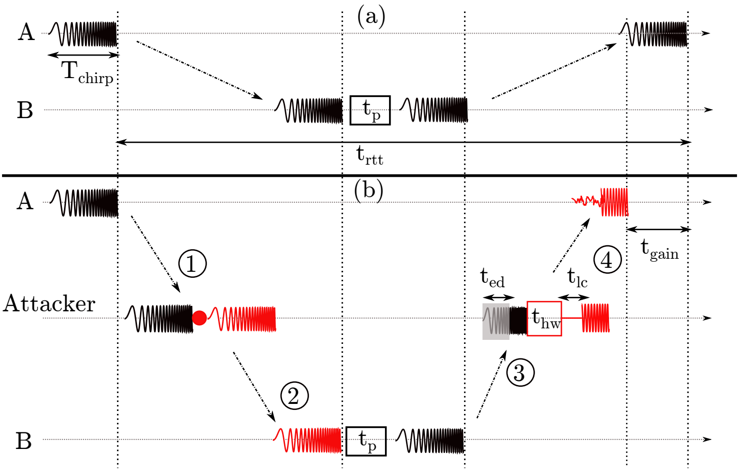
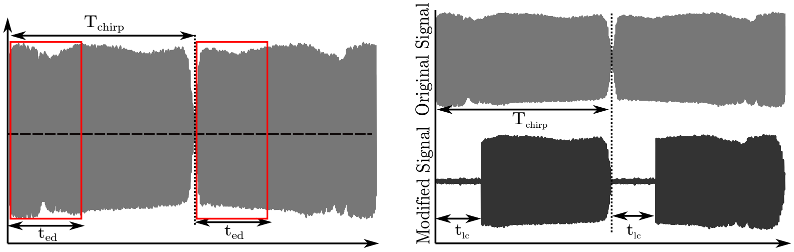


Figure 4.4: *Distance decreasing attack: (a) CSS ranging in a non-adversial setting where t_{rtt} is the estimated RTOF. (b) Attacker reduces the total round-trip time to $t_{rtt} - t_{gain}$ by performing early detect and late commit on node B's response CSS signal while communications from A to B are relayed without any LC or ED.*

The distance-decreasing relay attack is performed by an external attacker under the assumption that devices A and B are both honest. To decrease the distance, it is insufficient for an external attacker to simply relay signals between the devices as the round-trip time would still be equivalent to the actual distance between A and B. Instead, a successful attacker must Early Detect (ED) signals from A and Late Commit (LC) those signals to B. Clulow et al. [39] introduced attacks using ED and LC and their feasibility on RFID was demonstrated in [68]. Here, we study the feasibility of ED and LC attacks on CSS-based ranging. We assume the attacker is able to receive signals over the entire bandwidth necessary and has knowledge of system parameters including the modulation scheme, symbol duration, and packet structure.

Figure 4.4 illustrates how an attacker modifies the distance by means of early detect and late commit of CSS signals. Figure 4.4(a) shows CSS ranging in a non-adversarial setting, where t_{rtt} denotes the time taken to receive a reply from device B for a ranging signal transmitted by A and t_p is B's processing time. The distance between A and B is computed using the expression $\frac{c \cdot t_{rtt}}{2}$.

Figure 4.4(b) shows an attack on CSS ranging by ED and LC. We assume that the attacker is closer to A than B is. The attacker first receives the signal



(a) *Signal properties of early detect.*

(b) *Signal properties of a late committed signal.*

Figure 4.5: *ED and LC signal structure: (a) Early detect: t_{ed} is the time period over which the CSS signal is observed before predicting the symbol. (b) Late commit: An arbitrary signal (here just channel noise) is transmitted for a time duration t_{lc} before committing to the correct symbol.*

transmitted by A, amplifies it and forwards it to B (1). B receives, demodulates, computes the response and transmits the response back after a time delay t_p (2). The attacker now "early detects" the response (3). For early detection, the attacker modifies the receiver circuits to determine the symbol's data earlier than a standard receiver. Let $t_{ed} < T_{chirp}$ be the time required to predict the symbol with a high confidence; T_{chirp} is the time duration of a single chirp signal, i.e., symbol duration. Simultaneously with the early detection phase, the attacker performs a late commit attack. It consists of first transmitting an arbitrary signal (e.g., any signal with zero correlation with the up- or down-chirp) during the early detection phase. Once the symbol is predicted, the attacker stops transmitting the arbitrary signal and switches to transmitting the chirp corresponding to the predicted symbol, i.e., the attacker *commits* to the predicted symbol, commonly known as a late commit. Let t_{lc} be the time duration for which the arbitrary signal is transmitted until the correct symbol has been predicted. The early detection of chirps and the late commit signal structure are shown in Figure 4.5a and 4.5b respectively.

The attacker hardware circuitry for performing the early detection and late commit introduces an inherent delay t_{hw}. The attacker transmits the chirp corresponding to the predicted symbol which A receives after a total round-trip time $t_{rtt} - t_{gain}$ thereby gaining a distance of $d_{gain} = \frac{c \cdot t_{gain}}{2}$. The effective time gained t_{gain} depends on three factors: (i) the minimum time window t_{ed} required to observe the chirp for early symbol prediction (ii) the maximum time t_{lc} the attacker can delay before committing to the correct symbol without introducing additional bit errors at the receiver (iii) the attacker's hardware delay t_{hw} required for symbol prediction and symbol retransmission. The effective time gain is calculated as follows.

$$t_{gain} = t_{lc} - t_{ed} - t_{hw} \tag{4.4}$$

In the following subsections, we discuss how to perform the aforementioned early detection and late commit attacks on CSS based ranging systems. In Section 4.4.3, we validate these attacks experimentally.

4.3.2 Early Detection of CSS Signals

We propose two ways of predicting CSS signals without requiring the receiver to receive the entire chirp: (i) zero crossing detection and (ii) early correlation using dispersive delay lines.

Zero crossing detectors: Zero crossing detectors detect the transition of a signal waveform through zero level. The basic idea of using zero-crossing detectors to perform early detection is that a low-frequency signal has fewer such transitions than a high-frequency signal for a fixed time window. As explained in the previous sections, an up-chirp (down-chirp) is a signal whose frequency increases (decreases) with time. Exploiting this property, we observe the signal over a time window much shorter than the chirp duration T_{chirp}. The number of zero crossings is then compared to template chirps and the symbol (bit) value is predicted. Under real-world conditions, channel noise increases signal transitions at the zero mark and thereby reduces prediction accuracy. However, our experiments on signals acquired under real channel fading show that setting a non-zero threshold value improves the symbol prediction accuracy. We were able to early detect by observing at least 20% of the chirp duration. Further details are provided in Section 4.4.3.

Early correlation with dispersive delay lines: Dispersive delay lines are electro-mechanical devices where the delay experienced by the signal in the line is proportional to its frequency. An input signal to the delay line is separated into its frequency components and results in a compressed pulse at the output. Radar systems used Surface Acoustic Wave (SAW) filters for pulse compression. Bulk acoustic wave filters have a higher operation bandwidth with delays in the range of $0.5 - 2.5\mu$s. It is, therefore, possible to implement a short-time correlator for the start frequencies of the chirp without the need of digitizing the signal. This procedure would “early detect” the chirp structure (up- or down-chirp) by producing an output at the appropriate delay line.

In the digital processing domain, this is analogous to a short-time correlator where we only correlate part of the template chirp signal before predicting the bit. We performed such experiments on signals captured over real channels. Our results indicate that it is possible to predict early by correlating over only 5% of the chirp duration.

4.3.3 Late Commit of CSS Signals

In a late commit attack, the attacker transmits an arbitrary signal that is constructed based on the receiver's implementation of signal detection and interpretation until the correct bit is available. Since CSS receivers implement matched filters that decode the symbols by cross-correlating the received signal with known template chirps, optimal late commit results are obtained if the attacker does not transmit any signal until the correct symbol is available, i.e., if the attacker's arbitrary signal is a "zero" signal. In order to maximize the effectiveness of the attack, i.e., maximize distance decrease, it is important for the attacker to know its distance from B. Based on this distance, the attacker can time its start of transmissions. Figure 4.5b shows the modified and unmodified signals (2 symbols) as received by the receiver. t_{lc} is the period for which the attacker does not transmit any signal while deciding on the correct chirp signal to be transmitted. We show by simulations in Section 4.4.3 that the receiver is still able to decode the modified signal with an acceptable bit error rate.

4.4 Experimental Evaluation

In this section, we first describe our simulation and experimental setup. We then evaluate the feasibility of ED and LC attacks using simulated and recorded signals from a COTS transceiver in an indoor environment. Finally, we summarize the attacker's distance advantage for several chirp durations.

4.4.1 Experimental Setup

Our simulation and experimental setup (Figure 4.6) consists of a simulated chirp transmitter, a COTS chirp-based ranging transceiver and a chirp receiver able to process both simulated and recorded chirp transmissions.

Simulated chirp transmitter: The parameters to simulate the transmitter, i.e., packet structure, data encoding, chirp duration and bandwidth, and carrier frequency were chosen based on the available documentation in the standards and monitoring signals of the NanoLOC transceiver. The transmitter block

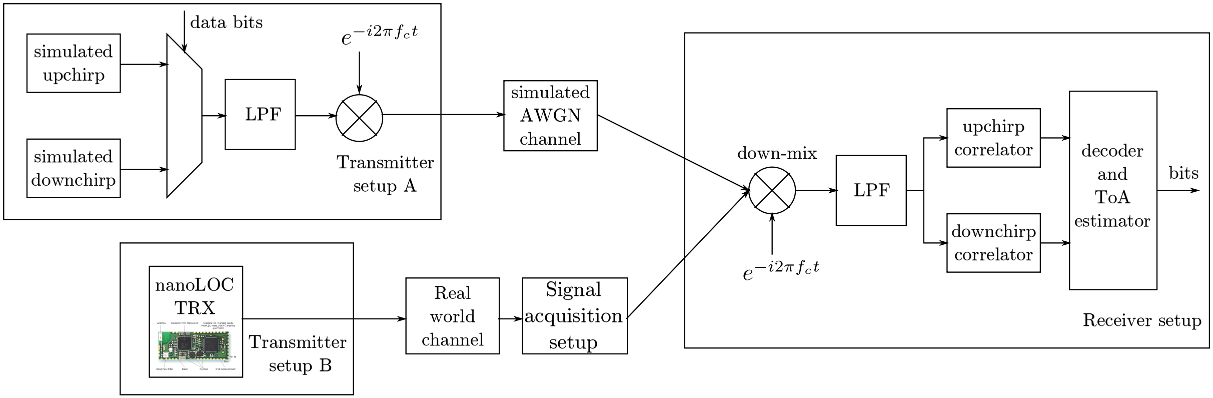


Figure 4.6: *Experimental setup consisting of the simulated chirp transmitter (Transmitter setup A), the NanoLOC transceivers (Transmitter setup B) and the CSS receiver.*

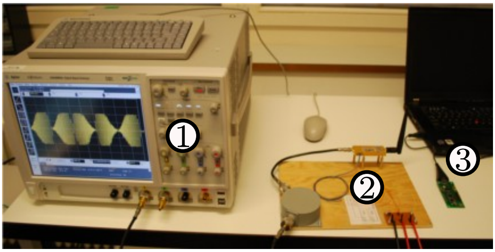


Figure 4.7: *The signal acquisition setup for recording NanoLOC transceiver CSS transmissions. (1) Digital storage oscilloscope. (2) Amplifier and receiving antenna. (3) NanoLOC transceiver.*

consists of a chirp generator, a low-pass filter and a mixer. Data bits are encoded using the BOK scheme. One data packet contains 256 bits with 20 bits of alternating 0s and 1s as preamble and a 64 bit sync word. The chosen sync word is same as the one used in the NanoLOC transceiver. The remainder of the data packet consists of a MAC frame, payload, and CRC checksums. The chirp duration T_{chirp} (corresponding to one data bit) is varied within the set $T_{chirp} = \{1, 2, 4\}$ μs. The baseband complex chirp signal is quadrature modulated with a 2.441 GHz carrier before transmission. The transmitted CSS signal is subject to additive white gaussian noise with varying signal to noise ratios. Table 4.1 lists the various system parameters and their corresponding values chosen for the experimental evaluation.

NanoLOC transceiver: In a real-world communication, the wireless channel causes multiple signal impairments that adversely affect the communication and ranging accuracy. We validate our attacks under real-world channels using the NanoLOC transceiver. It is programmed to continuously transmit a known payload data. The receiver later uses this knowledge to estimate the bit errors. The chirp duration T_{chirp} is set to 2μs. The NanoLOC is positioned at various locations and at different distances from the receiver setup to capture different channel realizations. The setup used for capturing the NanoLOC's transmissions is shown in Figure 4.7. The captured signal measurements are later used to determine two characteristics under real-world channel effects: (i) an attacker's ability to early detect a chirp (ii) the correctness with which an honest receiver decodes a late-committed CSS signal.

Receiver setup: The receiver consists of a quadrature demodulator, low-pass filter and matched filter blocks implemented in Matlab. The quadrature demodulator converts the received CSS signal to its baseband complex signal. The matched filters correlate this signal with the template up- and down-chirps. The output of the matched filters is compared and the received bit is decoded. To capture the NanoLOC transmissions, we use an additional signal acquisition setup. This setup consists of a horn antenna for better directionality and a $40\,\mathrm{dB}$ low-noise amplifier. The received signal is then digitized at RF by an oscilloscope where the data is sampled at $10\,\mathrm{GSa/s}$ and stored. Figure 4.8 shows the received signal under an AWGN channel and real-world channels in comparison to the originally transmitted chirp. In reality, radio signals experience fading as they propagate through the channel to the receiver. Certain frequencies get attenuated more than the others as signals traverse multiple paths to reach the receiver. This effect is observed in the NanoLOC signal recordings at a distance of $2\,\mathrm{m}$ as shown in Figure 4.8.

4.4.2 Evaluation Metrics

We evaluate the effectiveness of the attacks based on the number of errors introduced at the receiver due to ED and LC modifications of the CSS signal. The decoded bits are compared with the originally transmitted bits and the number of bit errors per packet computed. We indicate the bit error rate as a percentage of the transmitted packet size of 256 bits. In the case of AWGN channel, the evaluations were averaged over 100 different iterations for each SNR value in the set $5, 10, 15, 20, 25$ dB. For the experiments performed using the NanoLOC transceiver, the device was positioned at several indoor locations and at varying distances of 1, 2, 3, 5, 10 and 18 meters away from the receiver. We collected 10 sets of traces at every location with each trace containing two 256 bit packets using a digital storage oscilloscope.

4.4.3 Experimental Results

In this section, we present the results of ED and LC attacks performed on CSS signals. We also evaluate these attacks when error correcting codes are used and summarize the maximum distance decrease achieved.

Early detection of chirps: We evaluate the feasibility of early detection using the zero crossing detector and short correlations (Section 4.3.2).

Our implementation of zero crossing detector-based early detection consists of a counter and comparator. We assume the attacker knows the number of zero crossings that occur within a specified time window for a standard up- or down-chirp. t_{ed} is the time window over which the transmitted signal is observed. The counter contains the number of zero crossings that occurred over

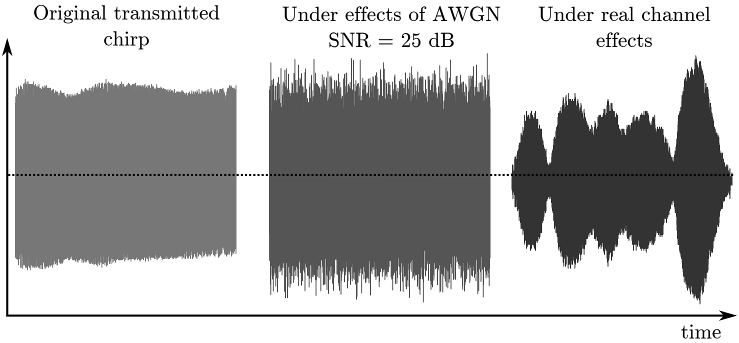


Figure 4.8: *Comparison of the received CSS signal under an AWGN channel and real-world channels with that of the originally transmitted chirp.*

Parameter	**Value**
Simulated Transmitter (A)	
T_{chirp}	1μ s, 2μ s, 4μ s
f_c	2.441 GHz
ω_{BW}	80 MHz
$Packetlength$	256 bits
NanoLOC TRX (B)	
T_{chirp}	2μ s
f_c	2.441 GHz
ω_{BW}	80 MHz
$Power_{dBm}$	0 dBm
$Packetlength$	256 bits

Table 4.1: *System parameters used in the analysis.*

the time t_{ed}. The symbol is predicted by comparing the counter value against the expected values for up- and down-chirps over the time t_{ed}. Figure 4.10a shows the number of incorrect predictions for various time window sizes (t_{ed}). We were able to achieve a 100% prediction accuracy when observing every chirp for t_{ed} values from 20% to 80% of T_{chirp} for an SNR of 25 dB under AWGN channel. Under real-world channels, where the CSS signal experiences fading, we were still able to predict with 100% accuracy for t_{ed} values from 20% to 70% of T_{chirp}. This is shown in Figure 4.10b. The increase in symbol errors or decrease in prediction accuracy for higher values of t_{ed} is due to the chirp signal property itself. An up-chirp has an increasing frequency

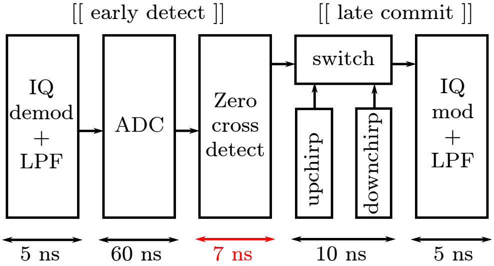


Figure 4.9: *Attacker hardware: The zero crossing detector algorithm tested on a FPGA introduced a delay of* 7 ns. *Specified time delays of other blocks are based on COTS hardware specifications.*

sweep while a down-chirp sweeps down the frequencies over the same band. Therefore, the number of zero crossings that occur over the entire duration of a single chirp T_{chirp} is equal for both the chirps. Hence, the number of symbol errors increases as $t_{ed} \rightarrow T_{chirp}$.

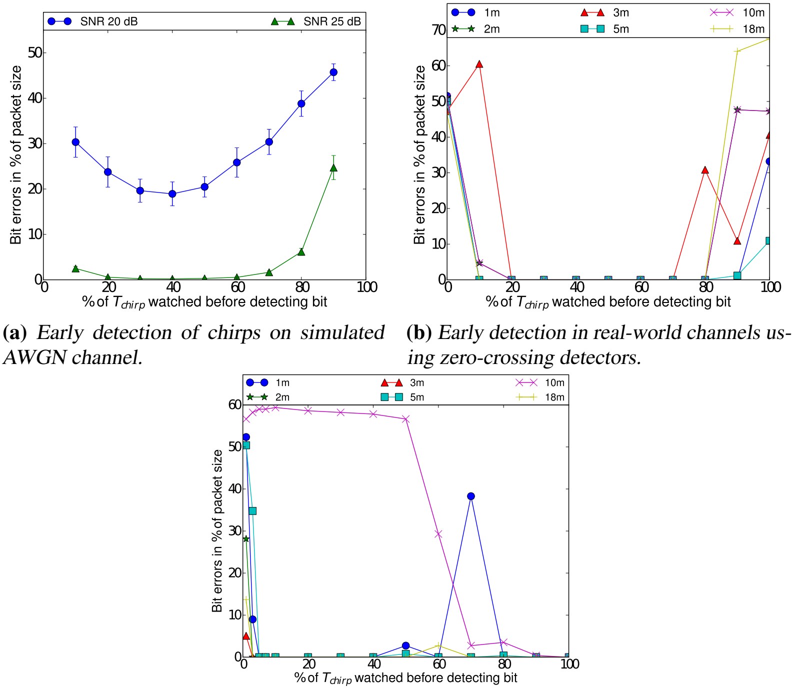
The noise introduces randomness in the number of signal transitions at the zero crossing and adversely affects the symbol prediction accuracy. A countermeasure is to use a non-zero value for detecting the transitions. In our implementation, the threshold value is configurable and is not limited to zero. We select the threshold value based on the noise floor level, which is estimated from channel observations in the absence of CSS transmissions.

Dispersive delay lines is an alternative design the attacker can implement to early detect chirp transmissions. As described in Section 4.3.2, this design is analogous to a short time correlator implemented in a DSP. In our experiments, we correlate the received CSS signal with a fraction of the template chirps, i.e., over a smaller time window (t_{ed}) of the original chirps. Our results indicate that it is possible to achieve 100% symbol prediction accuracy, cross-correlating only 5% of the received chirp even under real-world channels. The results are shown in Figure 4.10c. It is important to note that cross-correlation using a DSP introduces a delay of the order of few μs. The exact delays exhibited by dispersive delay lines in a completely analog implementation remain to be explored.

Late commit attack: We evaluated the behavior of the receiver under a late commit attack. To this extent, an arbitrary signal was transmitted for a time t_{lc} before switching to the appropriate chirp signal. We measure the receiver's ability to decode the symbols for varying t_{lc} and compute the number of symbol errors introduced due to the late-commit chirp signal. Figure 4.11a and Figure 4.11b show the number of symbol errors at the receiver for various hold times before committing the actual chirp, i.e., varying t_{lc}. The results indicate that at high SNR values, the receiver is able to decode all symbols when the attacker takes as long as 70% of T_{chirp} before committing to the correct chirp. We further evaluated the receiver's behavior under real-world channels. The receiver was able to decode all symbols for t_{lc} values up to 60% of T_{chirp}. In high SNR signal reception, the receiver tolerated t_{lc} values up to 80%. The results under the measured real-world channels are shown in Figure 4.11c.

Hardware implementation: The attacker's hardware delay influences the effective distance decrease. Figure 4.9 shows the building blocks of an attacker's hardware. The received signal is demodulated and sampled before feeding them to the zero crossing detector block for early detection. We implemented the zero crossing detector algorithm in VHDL and tested it on a Xilinx Spartan 3A FPGA board. The time taken for the algorithm (implemented in hardware) to predict the symbol from the moment all required samples from the analog to digital converter is available was 7 ns. The time delays of the demodulator, ADC, switch and the modulator shown in the figure are typical delays based on COTS components. The switch and the IQ modulators form part of the late commit hardware, which also contributes to the total hardware delay ($t_{hw} = 87$ ns). We account for t_{hw} in our effective distance decrease estimates described in Section 4.4.3.

Effect of error correction coding schemes: Errors in wireless communications, e.g., due to channel fading are common. Error correcting codes add redundant bits to the message before transmission to improve data communication reliability. The receiver uses this redundant information to detect or correct bit errors that occur during transmission. The NanoLOC transceiver can be configured to enable error correction and implements the $(7, 4)$ Hamming code. The linear $(7, 4)$ Hamming code [63] encodes 4 data bits into 7 bits by adding 3 parity bits. A scheme implementing the $(7, 4)$ Hamming code corrects single bit errors. Therefore a 256 bit packet including redundant bits appended by the data encoder, the receiver would still be able to recover the original message for bit errors up to 14% of the packet. With this information, we conclude from Figure 4.11c that it would be possible for an attacker to commit as late as after 90% of the chirp duration T_{chirp}. For early detection, the attacker could predict 10% of the symbols and yet mount a successful



(a) *Early detection of chirps on simulated AWGN channel.*

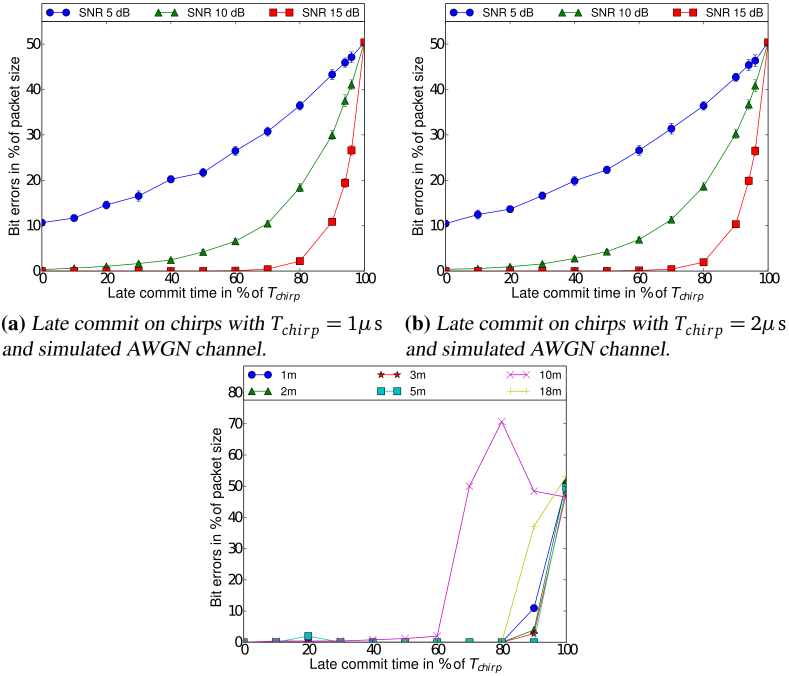
(b) *Early detection in real-world channels using zero-crossing detectors.*

(c) *Early detection in real-world channels by early correlation.*

Figure 4.10: *Early detection results: (a) Under a high SNR AWGN channel, it was sufficient to observe only* 20% *of chirp duration to predict the symbol. (b) Similar results for CSS signals received from the NanoLOC transceiver at various positions using zero-crossing detection. (c) Cross-correlating* 5% *of* T_{chirp} *is sufficient for predicting the symbol accurately for most channel conditions.*

distance decreasing attack. To this extent, from Figure 4.10b it would be sufficient to observe the chirp only for 10% of the chirp.

Effective distance advantage for an attacker: We summarize the effective distance advantage an attacker gains in executing the ED and LC attacks. We derive our distance decrease estimates based on the experimental results under real-world channels. As described in Section 4.3.1, the effective distance gained depends on three factors: (i) t_{ed} (ii) t_{lc} and (iii) t_{hw}. From Figure 4.10b,



(a) *Late commit on chirps with $T_{chirp} = 1\mu$s and simulated AWGN channel.*

(b) *Late commit on chirps with $T_{chirp} = 2\mu$s and simulated AWGN channel.*

(c) *Late commit under real channel effects*

Figure 4.11: *Late commit receiver behavior: (a & b) For high SNR AWGN channels, the attacker can take as long as 70% of T_{chirp} before committing to a symbol. (c) For most of the real-world channels in the experiment, the receiver decoded all symbols for t_{lc} values up to 80% of T_{chirp}.*

the attacker is required to observe at least 20% of the chirp period to predict the symbol with 100% accuracy. Similarly, from Figure 4.11c, an attacker can wait no longer than 80% of T_{chirp} for committing to a symbol. The attacker's hardware delay in Section 4.4.3 is 87 ns. The maximum distance decrease possible is calculated using the expression $d_{gain} = \frac{c \cdot t_{gain}}{2}$. The results and the parameters are summarized in Table 4.2. We conclude that an attacker would be able to successfully mount a distance decrease of more than 150 m for 1μs chirps and up to 700 m for 4μs long chirps. However, the use of error correcting codes increases the above estimates by about 10%.

Common Parameters	T_{chirp}	**Distance gained**
$t_{ed} = 20\%$ of T_{chirp}	1μs	153 m
$t_{lc} = 80\%$ of T_{chirp}	2μs	333 m
$t_{hw} = 87$ ns	4μs	693 m

Table 4.2: *Effective distance estimates.*

4.5 Discussion

Our analysis demonstrates the feasibility of physical-layer distance decreasing attacks on CSS ranging and their security implications. One countermeasure is to estimate the power spectral density (PSD) of the received CSS signal. PSD of a signal indicates the distribution of energy in the various frequency components of the signal. In a late commit attack, the attacker transmits an arbitrary or no signal until the correct symbol is predicted. Since chirp signals sweep all frequencies in a linear manner, a late commit attack results in missing frequency bands. The receiver may detect the attack based on the energy voids in the PSD. It is important to note that spectral estimation techniques are computationally intensive and so are unsuitable for ultra-low power ranging solutions. An alternative approach is to set a specific threshold on the compressed pulse peak amplitude. The output of the matched filter or the dispersive delay line is a compressed pulse which is an aggregation of the energy present in the received signal's frequency components. Thus, under a late commit attack, the peak amplitude of the compressed pulse would be lower and the receiver could detect this change by setting an appropriate threshold. While low-cost and simple to implement, the major issue with such a countermeasure is to distinguish between actual attacks and channel fading effects. Even in a non-adversarial environment, wireless signals experience fading as they propagate through the channel. Signal frequencies get attenuated which would also affect the peak amplitude. Therefore, setting a threshold needs to take into account the channel uncertainty in order to reduce the false positives, i.e., channels that attenuate the CSS signals in a similar manner as a late commit attack. Further investigation is required to evaluate under what conditions (e.g., SNR) this countermeasure would work in an effective way.

4.6 Related Work

Physical-layer security of wireless systems has gained a lot of interest in the last years. It exploits the physical properties of the radio communication system and is therefore independent of any higher level cryptographic protocols implemented. Several attacks ranging from simply relaying the signal between honest nodes to injecting messages at the physical layer were demonstrated in the past. In this section, we discuss relevant related work in the physical-layer security of wireless ranging systems beginning with the works closest to ours.

Clulow et al. [39] introduced physical-layer attacks such as early detect and late commit attacks. The feasibility of these attacks on a ISO 14443 RFID was demonstrated in [68]. Flury et al. [56, 110] evaluated the security of IEEE 802.15.4a with impulse radio ultra wide-band PHY layer. The authors demonstrated an effective distance decrease of 140 m for the mandatory modes of the standard. The evaluations were performed using simulations. The inherent hardware delays due to bit detection, antenna, and heterodyning circuitry were not considered. Poturalski et al. [109] introduced the Cicada attack on the impulse radio ultra wide-band PHY. In this attack, a malicious transmitter continuously transmits a 1 impulse with the power greater than that of an honest transmitter. This degrades the performance of energy detection based receivers resulting in distance reduction and possibly denial of service. Recently, Francillon et al. [57] demonstrated distance decrease attacks on passive keyless entry systems deployed in modern cars by relaying signals at the physical-layer between the key and the car using a USRP [3].

Chirp signals were initially used in radar systems. Due to their resilience towards channel interference, chirp signals were later proposed for use in spread spectrum communications [43, 153]. David Adamy in [17] describes ways to detect, jam, intercept and locate chirped signals and transmitters. The emergence of dispersive delay lines such as the SAW delay lines made it possible to realize less complex wideband pulse generators and detectors [94]. Recent increase in the number of ranging application requirements and the standardization of CSS in the IEEE 802.15.4a as an alternative PHY resulted in a number of CSS-based ranging schemes [18, 83, 101, 122]. Yoon et al. [155], performed an exhaustive experimental analysis of the NanoLOC ranging system under non-adversarial settings in both indoor and outdoor environment and discussed its implications. To the best of our knowledge, this work is the first that analyzes the security implications of CSS based ranging systems.

4.7 Conclusion

In this chapter, we demonstrated physical-layer attacks on chirp-based ranging systems. More specifically, we focused on distance decreasing attacks based on early detection and late commit of chirp signals. We proposed and evaluated several early detection mechanisms. We also analyzed the receiver's decoding and TOA estimation behavior to late commit attacks on the chirp signals. Our experimental results showed that an attacker can decrease the distance by more than $150\,\mathrm{m}$ for $1\mu\,\mathrm{s}$ chirps and approximately $700\,\mathrm{m}$ for $4\mu\,\mathrm{s}$ chirps. Nevertheless, the advantages provided by chirp signals specifically the ability to process them using analog signal processing blocks only makes them an attractive option for realizing low-power, low-complexity ranging systems. In the next chapter, we leverage this property of chirp signals and propose a novel distance bounding system that is suitable for power-constrained applications such as contactless authentication and access control systems.

Chapter 5

Secure Proximity Verification for Contactless Systems

5.1 Introduction

Contactless smart cards are used in a number of applications including public transport ticketing, parking and highway toll fee collection, payment systems, electronic passports, physical access control and personnel tracking. Smart card based physical access control and authentication are deployed even in safety- and security-critical infrastructures such as nuclear power plants and defense research organizations. The majority of these smart cards use radio frequency identification (RFID) technology to exchange information with the reader. Modern contactless payment systems use Near-field communication (NFC) technology, a branch of RFID that is specifically designed for ultrashort-range applications typically in the order of a few centimeters. Even though the communication range for many such systems is limited, prior research has revealed that the use of RFID proximity to provide access control is still vulnerable to mafia-fraud (relay) attacks (e.g., PKES systems [57], NFC phones [58], Google Wallet [121]). As mentioned previously, relay attacks have serious implications on contactless access control and authentication systems: an attacker can gain entry into a restricted area, steal a car or make fraudulent payments by relaying the communications between the reader and the card which is several meters away without the knowledge of the card's owner. In order to prevent such attacks, these systems must be enhanced with distance bounding [33] i.e., with the ability to securely verify a device's proximity to the verifying terminal or reader.

The use of distance bounding in contactless access control and authentication systems, however, imposes a number of challenges. First, the verifier should estimate the distance bound precisely. Existing RFID proximity systems were not designed for this purpose and due to their operating frequency and bandwidth cannot achieve the ranging precision required for the prevention of relay attacks. Second, the physical communication layer used for distance bounding has to be robust to attacks such as early detection and late commit [39]. Finally, it is essential that the hardware complexity of the contactless card is kept as simple as possible. It would be best if the card can operate passively (derive power from the interrogation signal) or semi-passively (assisted by a power source).

Additionally, with the advent of *Internet of Things* (IoT), a large number of interconnected sensors and actuators are expected to collect and exchange information. These *things* can be implanted heart monitors that send continuous data to the patient's mobile phone, automobile sensors monitoring tire pressure or a simple automatic indoor climate control system. Given the sensitivity and privacy of the data that is exchanged, it is only reasonable to allow data communication between devices that are in close proximity; thereby making it very important to develop low-complexity, power efficient distance bounding systems.

In this chapter, we propose a novel distance bounding system with a ranging precision and security guarantees that make it suitable for contactless access control and authentication applications. Our system is based on frequency modulated continuous wave (FMCW) for distance estimation and On-Off Keying (OOK) technique for data communication. We leverage backscatter communication to enable the realization of low-power provers that can potentially be integrated into passive and semi-passive contactless cards. We show that due to the inherent nature of FMCW, the distance estimation phase is only loosely coupled to the challenge processing at the prover i.e., the distance estimation is independent of the processing delay at the prover while keeping the security guarantees of the system intact. This enables logical layer implementation of any distance bounding protocol proposed in prior art. Our proposed system architecture offers complete protection against conventional distance modification attacks. In addition, we provide maximum distance reduction estimates for a strong attacker who is capable of detecting challenges earlier and relaying them to the payment token. We show that an attacker who can predict the symbol as early as 10 ns and can relay without any hardware delay can reduce the estimated distance by a maximum of 1 m. Finally, we evaluate our system through simulations and experimentally validate its processing delay, power consumption and ranging precision.

5.2 Contactless Smart Cards

Contactless smart card systems use radio frequency signals to communicate between the reader and the smart card. The card reader continuously transmits radio frequency signals from which the smart card derives energy for its operation. Then, the card modulates back its data on the radio signal which is detected and demodulated by the card reader. Typically, the contactless smart cards use amplitude shift keying or phase shift keying [15] to modulate the data back to the reader. Depending on the application and environmental factors, contactless smart card systems use different frequency bands for communications. The $124-135\,\mathrm{KHz}$ low-frequency and $13.56\,\mathrm{MHz}$ high-frequency (HF) bands are the most commonly used ones. Some systems also use the ultra-high frequency ($902-928\,\mathrm{MHz}$ and $860-880\,\mathrm{MHz}$) and the microwave bands ($2400-2483.5\,\mathrm{MHz}$ and $5725-5850\,\mathrm{MHz}$). Passive and semi-passive cards can operate in any of the above mentioned frequency bands while most active tags (can transmit autonomously and equipped with a power source) use the UHF or microwave frequencies for operation.

Contactless smart cards were first deployed in the mid 90's for electronic transport ticketing in Finland. Today, contactless smart card systems are used in securing access to critical infrastructure, contactless payments, electronic passports. The set of applications is only bound to increase especially given the recent advent of IoT. In a typical access control application, an authorised personnel simply taps his smart card against a card reader setup at the entrance to gain access to an infrastructure. In electronic ticketing, contactless smart cards are also used to store electronics funds of money. The customer can "top up" the card using cash or credit card at designated machines and later use it to pay for the public transport. A passenger simply taps the contactless smart against automated card readers while entering the public transport. The reader then checks for available balance in the smart card and deducts the appropriate fee. Similarly, in a typical electronic payment scenario, the consumer places the token very close to the payment terminal. In most cases, these contactless smart cards can be used even without removing them from ones wallet.

Relay Attacks: Prior research have demonstrated the vulnerability of contactless smart card systems to relay attacks also termed as "mafia fraud". In contrast to the protocol level exploits [27, 100], relay attacks [46] do not re-

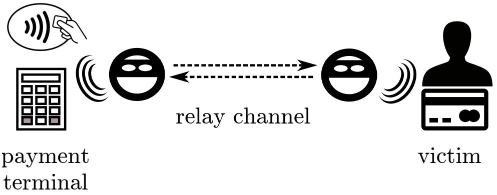


Figure 5.1: *An attacker relays the communications between a legitimate contactless payment terminal and a card using two proxy devices.*

quire any knowledge of the actual data being transmitted and therefore are independent of any higher layer encryption. A proxy reader and a proxy card are used to relay the communications between legitimate entities (Figure 5.1). Hancke [64] practically demonstrated the attack using specialized hardware as the proxy reader and card over a distance of 50 m. Later, Francis et al. [58] demonstrated that relay attacks can be executed using commodity phones equipped with NFC without the need for any specialized hardware. The proxy reader and token used Bluetooth as a proxy relay channel to exchange information between entities separated by several meters. Francillon et al. [57] showed the vulnerability of passive keyless entry systems implemented in modern automobiles to simple relay attacks. In this attack, the attacker used two devices, one each in the proximity of the key and the car. The attack was successfully executed by simply relaying messages between the key and the car, enabling the car to be opened and started even with the key at a distance of 50 m away from the car. Recently, [121] showed that relay attacks on Google Wallet can be carried out without any proxy hardware in close physical proximity to the victim. A "relay software application" communicates with the secure element present in Google Wallet and relays the information over the cellular network. In practice, the relay software application can be a malicious application which the user installed on his mobile device. The recently announced Apple Pay [1] uses NFC as the physical layer and hence also vulnerable to relay attacks[1].

Relay attacks can be prevented by implementing some sort of proximity verification e.g., distance bounding. In Chapter 2, we summarized and compared the state of the art in distance bounding implementations. We observed that all existing distance bounding designs, including the SCRCS design proposed in Chapter 3, require complex designs at the prover (in this case, the contactless smart card). For example, the designs proposed in [65, 136] require

[1] In some use cases, the authentication is based on TouchID, which has already been proven insecure [2].

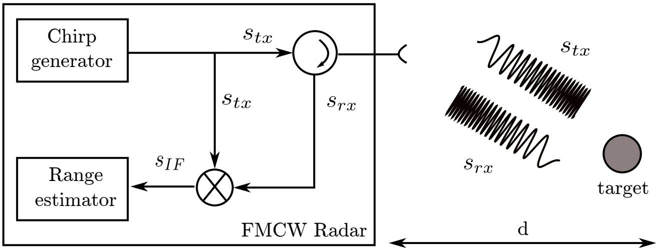


Figure 5.2: *Conventional FMCW-based radar system comprising of a chirp generator, mixer and a signal processing block to estimate range.*

the prover to transmit UWB impulses. Fast prover designs such as [115, 118] require the prover to receive and transmit using multiple frequencies. These limitations make them unsuitable for integration with many access control and authentication applications in which the prover (contactless card) is required to be fully passive. In this work, we fill this void by proposing a distance bounding system, specifically designed for use in contactless access control and authentication systems.

5.3 FMCW based Distance Bounding

5.3.1 FMCW Basics

Monotone (or single frequency) radars transmit pulses of short duration and measure distance based on the round-trip time of the received pulse reflected off the target. Such radars are more susceptible to channel interference. In a Frequency Modulated Continuous Wave (FMCW) radar [134], chirp signals [26] are used to determine range and velocity of a target. Figure 5.2 illustrates the basic building blocks of a conventional FMCW radar system. The radar base station transmits a chirp signal ($s_{tx}(t)$) which gets reflected off the target object back to the base station. The reflected signal ($s_{rx}(t)$) is then mixed with the transmitted signal at that instant to produce a “beat frequency”. The beat frequency (f_{Δ}) is proportional to the round-trip time (τ) taken to receive the reflected chirp signal; thereby able to measure distance d to the target object (Figure 5.3). The transmitted chirp signal $s_{tx}(t)$ is mathematically represented as shown below.

$$s_{tx}(t) = cos(2\pi f_{tx}(t)t) \tag{5.1}$$

where $f_{tx}(t)$ is the frequency sweep function given by Equation (5.2) and f_0 is the starting value of the frequency sweep. k is the rate of frequency sweep

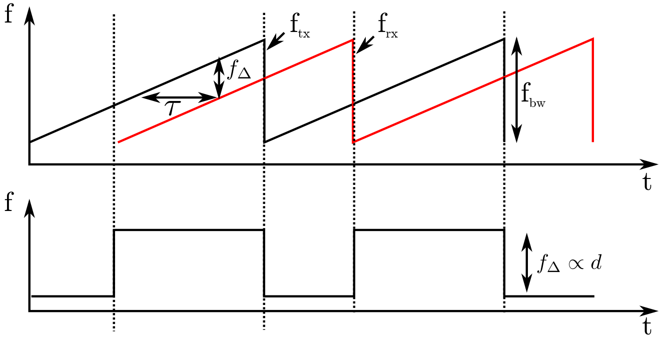


Figure 5.3: *Ranging principle: The beat frequency f_Δ is the difference between the instantaneous transmit frequency and the frequency of the reflected signal. This beat frequency is proportional to the round-trip time delay τ for the signal to be received after being reflected off the target object.*

and is a quotient of the length of the chirp signal T and the total bandwidth f_{bw} swept i.e., $k = f_{BW}/T$.

$$f_{tx}(t) = f_0 + kt \tag{5.2}$$

The transmitted chirp is reflected off the target object at distance d and is received back at the radar base station as $s_{rx}(t)$.

$$s_{rx}(t) = cos(2\pi f_{rx}(t)t) \tag{5.3}$$

The frequency of the reflected signal can be represented in terms of the instantaneous frequency of the transmitted chirp as

$$f_{rx}(t) = f_{tx}(t-\tau) = f_o + k(t-\tau) \tag{5.4}$$

Mixing the signals $s_{rx}(t)$ and $s_{tx}(t)$ results in an intermediate frequency signal $s_{IF}(t) = s_{rx}(t) \cdot s_{tx}(t)$ which consists of frequency components $f_{tx}(t) + f_{rx}(t)$ and $f_{tx}(t) - f_{rx}(t)$. The difference component is termed as the "beat frequency" given by

$$f_\Delta = f_{tx}(t) - f_{rx}(t) = f_{tx}(t) - f_{tx}(t-\tau) \tag{5.5}$$

Simplifying and representing τ in terms of distance d, i.e., $d = 2 \cdot \tau / c$, where c is the speed of light ($3 \cdot 10^8$ m/s), distance of the target object from the radar base station is estimated using Equation (5.7).

$$f_{\Delta} = k\tau = \frac{f_{bw}}{T} \cdot \tau \tag{5.6}$$

$$d = \frac{c \cdot f_{\Delta} \cdot T_s}{2 \cdot f_{bw}} \tag{5.7}$$

Maximum measurable distance and range resolution are two important performance metrics of any ranging system. Maximum measurable distance d_{max} is the largest value of distance d that can be measured using a particular ranging system. In an FMCW radar, this is dependent on the time duration T of the chirp signal and is given by $d_{max} = cT$. Range resolution δR is the minimum change in distance that can be detected and is proportional to the time resolution of $s_{tx}(t)$. In other words, δR is inversely proportional to the total bandwidth swept by the chirp and is mathematically represented as shown in Equation (5.8).

$$\delta R = \frac{c}{2 \cdot f_{bw}} \tag{5.8}$$

5.3.2 Data Modulation for Distance Bounding

Conventional radar systems do not require any kind of data transmission. However, in distance bounding protocols, the communicating entities (verifier and prover) exchange challenges and responses during the rapid bit-exchange phase. This requires data to be modulated over conventional FMCW radar signals. In this work, we modulate the challenge and response bits over the FMCW chirp signal using On-Off Keying (OOK). Mathematically, the transmitted signal with OOK modulation can be represented as

$$\sum_{n=1}^{N} c[n] \cdot \mathrm{rect}(t - nt_b) s_{tx}(t) \tag{5.9}$$

where t_b is the data-bit period given by $\frac{T}{N}$ (N is the length of the data packet to be transmitted) and $c[n]$ represents the payload. The distance bound is estimated similar to conventional FMCW radar systems based on the "beat frequency" f_{Δ} as shown in Equation (5.7). We describe the system design in more detail in the next sections.

5.3.3 Verifier and Prover Design

Figure 5.5 shows the high-level components present in our system. We focus on the rapid-bit exchange phase since it is, implementation- and power-wise the most demanding phase of the protocol execution.

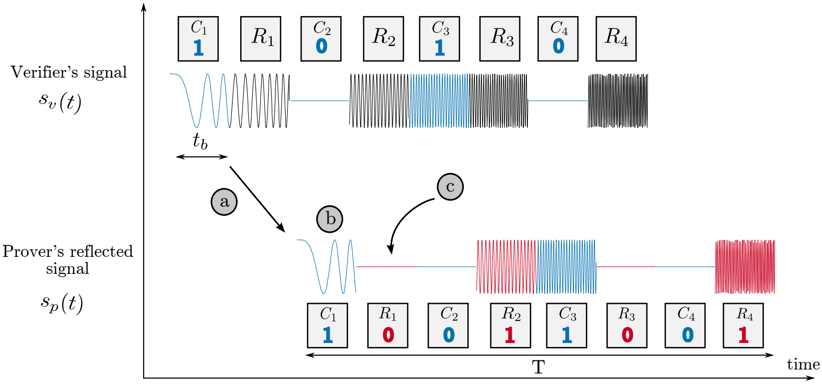


Figure 5.4: *An example signal as transmitted by the verifier (reader) and the corresponding reflected signal from the prover (contactless card). The shown signals are for challenge bits $c[n] = \{1, 0, 1, 0\}$ and the prover's processing function is a simple "invert" operation. The sequence of operation is as follows: (a) after propagation delay, the prover receives the interrogation signal, (b) the prover demodulates the challenge and computes its response. During this time, the prover continues to reflect the signal back, (c) after time t_b, during the response slot, the prover modulates back its response. The verifier and prover synchronize to these slots using a preamble (not shown in figure).*

The *verifier's transmitter* ($verifier\_tx$) module consists of an FMCW signal generator and an OOK modulator. The FMCW signal generator generates a chirp signal of time duration T. The entire chirp signal is divided into slots, each with time duration t_b. The prover synchronizes to these slots using a preamble that is transmitted by the verifier. The verifier divides the slots into challenge and reply slots such that every challenge slot is followed by a response slot. During the challenge slots, the verifier modulates the challenge bits using OOK modulation and continues to transmit the unmodulated chirp signal during the response slot (Figure 5.4). The response slots are used by the prover to transmit its response back to the verifier.

When the *prover* receives the challenge signal $s'_v(t)$ from the verifier, it demodulates the challenges and computes the response using a processing function. Any processing function proposed for distance bounding in the literature can be used here. It is important to note that the prover continues to reflect (backscatter) back the received signal while simultaneously demodulating the challenges and computing its response. The prover reflects the challenge unaltered but modulates the output of the processing function over

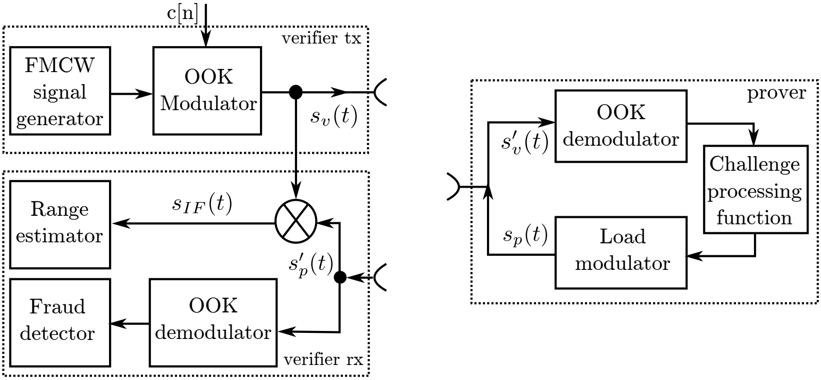


Figure 5.5: *OOK-FMCW based distance bounding system architecture: The interrogating signal $s_v(t)$ is an OOK-FMCW transmitted by the verifier. The prover receives, demodulates the challenge and computes the response while simultaneously reflecting the challenge signal back to the verifier. The responses are OOK modulated in the corresponding response time slot. The received signal at the verifier is then processed for both range estimation and verification of the prover's response.*

the response slot. Like in conventional passive RFID tags, the prover can simply load modulate its responses back to the verifier. We note that the propagation delay of the response computation path is one of the factors that determines the slot duration t_b.

The verifier's receiver module receives the reflected backscatter signal $s'_p(t)$ that contains the reflected challenges and the prover's modulated responses and estimates its distance to the prover. The verifier generates an intermediate signal $s_{IF}(t)$ by mixing $s'_p(t)$ with $s_v(t)$ as shown in Figure 5.5 and computes the range by analyzing the frequency components of $s_{IF}(t)$. In addition, the verifier demodulates and checks the correctness of the prover's responses. A key advantage of our FMCW-based distance bounding is that the range is estimated based on a "beat frequency" generated by mixing (analog) the received backscatter signal with that of the transmitted signal. It is sufficient that the verifier's sampling rate matches the beat frequency (which is typically tens of KHz) and not the entire sweep bandwidth; thereby reducing the verifier's design complexity.

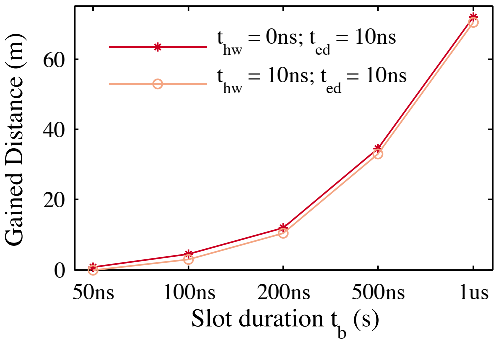


Figure 5.6: *Maximum distance an attacker can cheat by performing an early-detect and late-commit attack on the physical layer of the symbol.*

5.4 Security Analysis

In this section, we analyze the security of our proposed system against relay attacks (mafia frauds), distance and terrorist fraud attacks.

5.4.1 Mafia Fraud

There are two ways in which an attacker can carry out a mafia fraud at the physical layer: (i) Amplify and forward (ii) Early-detect and late commit of data symbols.

Amplify and forward: In this method, the attacker simply amplifies and relays communication between the reader and the contactless smart card. The attacker does not modify any physical layer characteristic of the symbol. Since the effective distance is computed based on the round-trip time delay, such an attack methodology would still result in the reader estimating its true distance from the victim's smart card. Alternatively, in conventional FMCW radar systems, an attacker can take advantage of the maximum unambiguous range parameter i.e., the largest value of distance d that can be measured unambiguously. In an FMCW radar, this is dependent on the time duration T of the chirp signal and is given by $d_{max} = cT$. An attacker can simply delay the backscatter response by more than the time duration T of the chirp signal and cause the system to estimate an ambiguous distance. However, in our design, since the FMCW chirp signal also contains OOK modulated challenges and responses, any ambiguity in the distance estimates will be detected.

Early-detect and late-commit: Clulow et al. [39] introduced the early-detect and late-commit attacks where a successful attacker early detects (ED) the symbols from the verifier and late commits (LC) those signals from the prover back to the verifier. The feasibility of ED and LC attacks on RFID was demonstrated in [68]. Here, we analyze the resilience of our proposed system against ED and LC attacks. In order to successfully execute the attack, the attacker must do the following: (i) early-detect the challenge from the reader, (ii) communicate/forward it to the contactless smart card, (iii) early-detect the response from the smart card and finally (iv) late commit a value back to the reader. For the analysis, let us consider one challenge and response slot. Assuming that the reader requires at least 50%[2] of the symbol to demodulate correctly, an attacker has $t_b + 0.5t_b$ time to respond. Within this time, the attacker must perform the above-mentioned operations. If t_{ed} is the time necessary for the attacker to reliably early-detect the challenge from the reader and the response from the victim's smart card, t_{hw} is the delay at the attacker hardware for amplifying and relaying, the time remaining for the attacker to relay communications is given by,

$$t_{mafia} = 1.5t_b - 2t_{ed} - t_{hw} \tag{5.10}$$

Since the contactless smart card is trusted (i.e., not tampered with), the response will be available only after the challenge slot time period i.e., t_b. Therefore,

$$t_{mafia} = 0.5t_b - 2t_{ed} - t_{hw} \tag{5.11}$$

Hence, the maximum distance an attacker can cheat on can be expressed as,

$$d_{gain} = \frac{c}{2} \cdot (0.5t_b - 2t_{ed} - t_{hw}) \tag{5.12}$$

It is important to note that Equation (5.12) holds good even in the scenario where an external attacker (in close proximity to the verifier) reflects the challenge signal back to the reader resulting in a beat frequency corresponding to the attacker's distance from the reader. However, for a successful attack, the attacker still has to modulate the response after the challenge slot period t_b. This time-constraint forces the attacker to early detect, relay and late commit the challenge and response bits as described previously and hence the maximum distance gained remains unchanged.

[2] This can vary depending on the type of receiver used to demodulate data. Hence we assume an energy detection based demodulator at the verifier with the threshold set to half the maximum symbol energy.

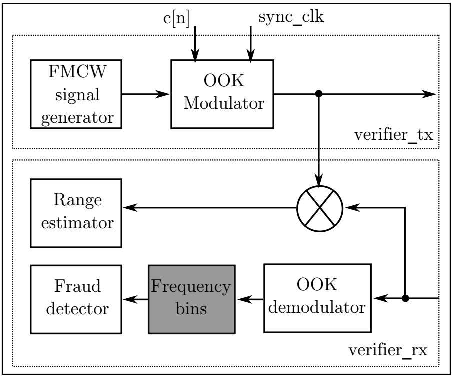


Figure 5.7: *Improved verifier design including the frequency bin based late-commit mafia fraud detector.*

The values for t_{ed} and t_{hw} depend on various characteristics of the attacker hardware (e.g., filter order, ADC delays, signal group delay, algorithm used to early-detect etc.) and t_b is selected based on the delay of the challenge processing function at the contactless smart card token. For example, a processing delay of 25 ns at the contactless smart card (Section 5.5.3) allows the t_b to be chosen at 50 ns. Assuming that the attacker is capable of detecting the symbol within $t_{ed} = 10$ ns and has ideal hardware ($t_{hw} = 0$), it is impossible to reduce the distance by more than 1 m in our system. In Figure 5.6, we give an intuition by substituting nominal values for t_{ed} and t_{hw}.

The effect of ED and LC attacks can further be limited by implementing the following two countermeasures: (a) Frequency bin analysis and (b) Phase modulation of responses.

Frequency bin analysis: The linearly increasing frequency characteristic of the chirp signal makes it feasible to detect mafia fraud attacks by analyzing the frequency components at specific time intervals. This temporal knowledge of the signal enables us to assign every challenge and response to one or more frequency bins. Each frequency bin contains spectral energy values for a range of contiguous frequencies. Specifically, it is possible to estimate the range of frequencies a particular challenge or response bit will occupy given a slot period t_b, starting sweep frequency f_0 and chirp duration T. We divide each challenge and response slot into N frequency bins. For a successful attack, the attacker must ED and LC every challenge and response. A late commit on a symbol would result in incorrect bin values and this would appear consistently throughout the chirp sweep bandwidth. Thus, by analyzing the frequency bins for expected spectral energy values, a late commit attack can be detected.

Phase modulation of responses: Another way to protect against ED and LC attack is by using phase modulation at the prover to communicate back the responses. It is widely known that a phase modulation receiver hardware is more complex than amplitude or frequency modulation receivers. Since, we use phase modulation *only to transmit* back the response, the hardware complexity of our proposed prover design does not increase significantly. Moreover, the ISO 14443 [15] standard for contactless smart cards allows BPSK modulation of a tag's responses. Unlike in amplitude or frequency shift keying techniques, it is difficult to predict the phase information of a received symbol before receiving it. Therefore, ED and LC attacks can be eliminated by modulating the challenges using OOK and the responses using phase.

5.4.2 Distance and Terrorist Frauds

In a distance fraud, an untrusted prover claims to be at a distance closer than the actual one. In conventional secure ranging systems, an untrusted prover can shorten the measured distance either by modifying its internal processing delay time (e.g., using improved hardware) or by replying before receiving the complete challenge signal (e.g., early detect and late commit attack). In our system, the dishonest prover does not gain any distance advantage by speeding up response computation, as the distance is estimated solely based on the beat-frequency created by mixing the reflected signal with the transmitted FMCW signal. The slot assignment to challenge and response bits forces the prover to wait until the challenge is reflected before modulating the response on the response slot. Early modulation would corrupt the challenge signal thereby being detected at the verifier during the response validation phase. Also, the prover does not gain any distance by executing such an early response attack as the distance estimation based on FMCW is decoupled from the data response at the prover.

In terrorist fraud attacks, an untrusted prover collaborates with an external attacker (without revealing his long-term secret) to convince the verifier that he is closer than he really is. Terrorist fraud resilient protocols [82, 120, 141] bind the prover's long-term secret to the nonces that are exchanged in the protocol thereby preventing the prover from revealing the nonces to the attacker. Since our proposed system is independent of the high-level protocol, the system security depends on the distance bounding protocol implemented above the physical layer.

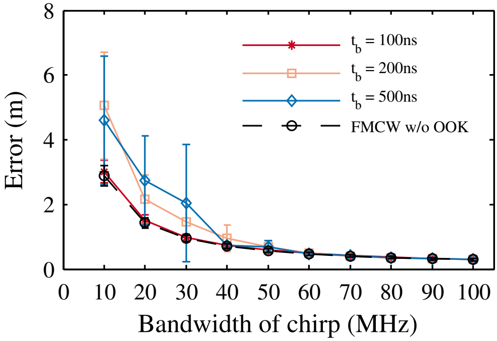


Figure 5.8: *Measurement precision: The mean error in distance estimation against bandwidth of the FMCW signal for various slot durations t_b. The SNR was fixed at* 15 dB *and the error is a mean value obtained by measuring 100 different distances within the possible maximum measurable distance.*

5.5 System Evaluation

In this section, we evaluate our proposed distance bounding system using both simulations and experiments. Through simulations, we analyze the bit error rate and ranging precision due to the on-off keying over FMCW. Then, we experimentally validate our prover's processing delay and ranging precision using a prototype.

5.5.1 Simulation Model and Analysis

The preliminary analysis through simulations were done using Matlab. The OOK-FMCW signal is generated by mixing a binary data signal with a chirp. The duration of a single chirp (T) was fixed at $10\,\mu s$ with the initial sweep frequency f_0 set to 2.4 GHz. The physical layer parameters such as the chirp bandwidth f_{bw} and bit-period (duration of each slot) t_b is made configurable based on the analysis performed. The generated OOK signal is passed through an additive white Gaussian noise (AWGN) channel. The signal to noise ratio (SNR) of the channel is varied depending on the analysis performed. We model the receiver as two submodules: (i) Energy detector for demodulating data sent over OOK-FMCW and (ii) FMCW-based distance measurement module. For the energy detection, the threshold value to distinguish the bits 0s and 1s is set at a value 6 dB lower than the maximum energy estimated for a 1 bit under no noise conditions. The signal processing for distance estimation is

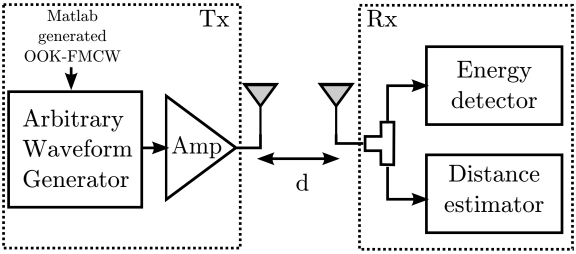


Figure 5.9: *Block level overview of the experimental setup comprising of the transmitter and receiver modules.*

implemented following the theory described in Section 5.3.1.

BER and Ranging Precision: First, we determine the minimum SNR required to reliably communicate data i.e., challenges and responses with the proposed physical layer scheme. In our simulations, we vary the SNR from 0–10 dB keeping the slot length $t_b = 100\,\text{ns}$ a constant. It is observed that for SNR greater than 8 dB, we were able to demodulate the bits with a BER of 10^{-7}. Next, we analyze the effect on ranging precision due to the OOK modulation over conventional FMCW radar. In addition to T, SNR is set to a constant 15 dB. For a specific t_b, the error in distance measured is determined for various values of f_{bw}. The error is a mean value obtained by measuring 100 different distances within the possible maximum measurable distance d_{max}. The simulations are repeated for $t_b = \{100\,\text{ns}, 200\,\text{ns}, 500\,\text{ns}\}$ and the results are shown in Figure 5.8. It is observed that the challenge slot period t_b has limited effect on the distance measurement precision for signals with bandwidth greater than 50 MHz. We note that, even at lower bandwidths, the observed precision would still be suitable for a variety of ranging applications. Alternatively, we could use amplitude shift keying e.g., a signal with low amplitude can represent a '0' bit as against absence of the signal itself (as in OOK). We use the above results of our preliminary simulations to build and evaluate our prover through real experiments.

5.5.2 Experimental Setup

Our experiments primarily focus on the two critical parameters of any distance bounding system: (i) Challenge processing delay and (ii) Ranging precision. A picture of our experimental setup is shown in Figure 5.10. The transmitter consists of an arbitrary waveform generator (AWG), a 20 dB radio frequency amplifier and a directional planar antenna. The OOK-FMCW signals are

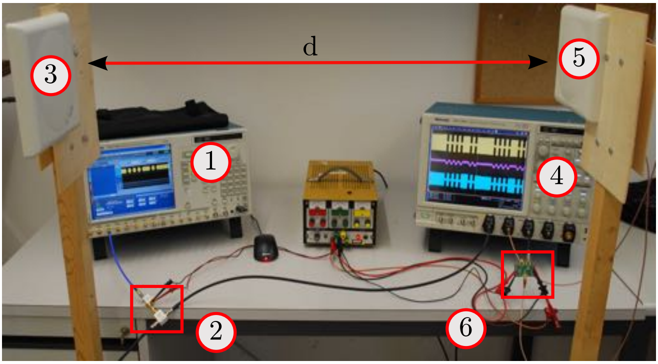


Figure 5.10: *An arbitrary waveform generator (1) outputs the OOK-FMCW samples. The signal is amplified (2) and a part of it is transmitted using a planar antenna (3) and the other recorded for distance estimation using a storage oscilloscope (4). The received signal (5) is input to the OOK detection and inverter circuit (6) and to the storage oscilloscope.*

generated using Matlab as described in Section 5.5.1 and loaded into the AWG. The OOK-FMCW signals are amplified and transmitted using a planar antenna. At the receiver, the signals are captured using a planar antenna similar to the one used at the transmitter. The received signal is recorded on a digital storage oscilloscope. In addition, the received signal is input to the challenge demodulator circuit [90] which essentially is a Schottky RF peak detector with programmable gain and a high-speed comparator with a built-in inverted output circuitry. The output of the demodulator circuit is also observed on the oscilloscope. We evaluate our system for different configurations of OOK-FMCW signals with the initial sweep frequency f_0 set to 2.4 GHz. We vary the FMCW signal's sweep bandwidth f_{bw} (100, 200 MHz), the slot period t_b (100, 250 ns) and the modulation index (75, 100 %). The energy detector consumed 2–3 mA current with a voltage bias of 3 V (6–9 mW power). The power consumption can further be reduced to hundreds of microwatts by using a slower detector and phase modulation for the card responses to prevent ED and LC attacks. We note that in our experimental setup, the oscilloscope just emulates the reader and our system does not require high sampling rates at the card (backscatters the challenges and responses) or the reader.

Parameter	Value
Sweep bandwidth f_{bw}	$100, 200$ MHz
Slot period t_b	$100, 250$ ns
Modulation index	$75, 100$ %

Table 5.1: *Different configurations of the signals used in the experimental analysis.*

5.5.3 Experimental Results

Challenge Processing Delay t_p: The challenge processing delay t_p plays an important role in deciding the duration of the challenge and response slots t_b. In our experimental setup, t_p is the time delay for the energy detector to demodulate the received OOK-FMCW challenge signal and invert the challenge signal. For accurate time delay measurements, the signals are pre-processed by applying Hilbert transform and passing it through a median filter (to preserve the rising and falling edges while reducing noise). Figure 5.11a shows the response times observed at the receiver over a number of trials. The processing delay was measured with the receiver placed at 1 and 4 m away from the transmitter. The medial delay observed was about 19.5 ns and remained largely unaffected by the distance from the transmitter. Hence, the value of t_b can be further reduced to about 50 ns (including fall-time) without affecting the decoding of challenge bits. Additionally, it is observed that the t_p values show greater variance with distance due to the variations in the received signal's energy between trials.

Ranging Precision: In order to evaluate the ranging precision, we placed the receiver at distances 2, 3 and 4 m from the transmitter. The distance bound is calculated using standard FMCW techniques as described in Section 5.3.1 and the results are plotted in Figure 5.11b. It can be observed that our prototype has a ranging precision of less than a meter for the evaluated short distances. A combination of factors such as range resolution δR (and hence signal bandwidth), channel multipaths and receiver sensitivity affect the precision of a ranging system. Other physical characteristics of the OOK-FMCW signal such as modulation index, bit (slot) period t_b and duration of chirp T had no effect on the precision of the ranging system. As with any wireless communication system, multipath and other channel interferences are additional factors that affect system performance. The robustness of FMCW to multipath interferences have been evaluated in [89]. The results illustrate that for an allowed

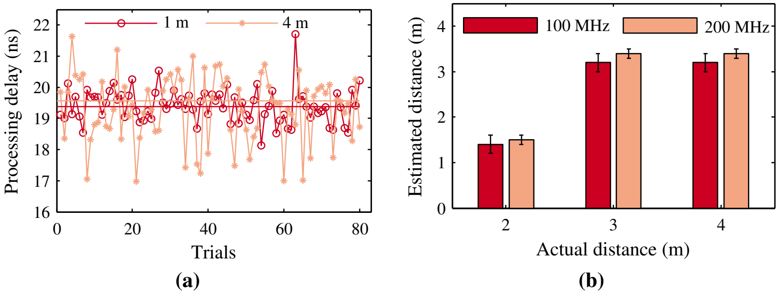


Figure 5.11: *(a) Challenge processing delays. The median value of* t_p *was approximately* 19.5 ns *for both the values of* $d = \{1\,\text{m}, 4\,\text{m}\}$*. (b) Ranging precision. For* $d = \{2, 3, 4\}$ m, *the errors in the estimated distances were less than a meter.*

ISM bandwidth of 80 MHz, the ranging uncertainty in a severe multipath environment was around 1 m and improved with higher sweep bandwidth.

5.6 Discussion

In this section, we discuss how the proposed FMCW-based distance bounding system can be integrated into state-of-art contactless smart cards to enable secure proximity verification. In addition, we briefly describe alternative design choices for the prover and the verifier in order to improve their robustness to attacks.

Modifications to modern contactless smart cards: The backscatter communication capability of modern contactless cards can directly be used to load modulate and reflect back the challenge and response. The only addition would be to incorporate the challenge detection and response computing function which can be as simple as a NOT or an XOR operation. There are already several commercially available radio frequency energy detectors [20, 90] with integrated comparators and amplifiers. In addition, the response time of these detectors are well under 100 ns and consume less than 3 mA of current. For example, the LTC5536 energy detector used in our experiments (Section 5.5.2) responds within 25 ns and can be easily integrated into can be integrated into modern contactless smart cards for an additional power consumption of less than 10 mW. Our design can be implemented in passive and semi-passive tags (e.g., [42, 128, 135, 147]) operating in the ISM 2.4 GHz and 5.8 GHz bands using 80 MHz and 150 MHz[3] bandwidth respectively to achieve high distance precision. Since our system targets short-range distance measurement applications (less than 5 m), the use of $6-8.5$ GHz spectrum [72] is also possible.

Distribution of Secret Keys: In our system, the terminal and the card need not share a secret key. Instead, it is sufficient that the contactless card and a central authority share a key, and that the terminal upper bounds the card's responses to its estimated range. The terminal can then communicate the card's response, the measured distance bound and the corresponding challenge to this central authority for validation during the transaction authorization phase of the payment protocol [48,49]. The above method is applicable even if the terminal is configured for offline transaction authorization.

Limitations: Our system leverages the ability of modern contactless cards to load modulate and reflect the challenge and response back to the verifier by means of backscatter communication. This enables the realization of low-power, low-complexity provers without the need for any specific transmission circuitry. However, the maximum distance between the verifier and the prover that can be measured depends on the ability of the verifier to receive and process this backscattered signal. Since the strength of the backscatter signals are typically weak and given the maximum allowable power in the ISM bands, the maximum distance the system can measure is limited to a few meters. Furthermore, our system can achieve a ranging precision of ≈ 1 m when operating in the ISM 2.4 GHz and 5.8 GHz bands that are most suitable for applications such as contactless payments and access control systems. More bandwidth is necessary for applications that require more precise ranging (e.g., cm-level) which can potentially increase the complexity of the system and hence the power consumption. There are already ranging system designs [135, 147] that can measure distances with a ranging precision of $15-30$ cm and a power consumption of $\approx 50-150$ mW.

5.7 Conclusion

In this work, we proposed a novel distance bounding system designed specifically for enabling secure proximity verification for contactless access control and authentication applications. Our system uses FMCW for distance measurement, on-off keying for data communication and backscatter property for realizing passive and semi-passive payment cards. We showed that our system

[3] In theory, 80 MHz gives distance resolution of 1.87 m, 150 MHz of 99 cm

is secure against various distance modification attacks and experimentally validated its performance.

Chapter 6

SPREE: A Spoofing Resistant GPS Receiver

6.1 Introduction

In the previous chapters, we mainly focussed on analyzing and designing secure proximity verification systems. In addition to proximity, the exact location is critical to a large number of applications. Today, a number of security- and safety-critical applications rely on Global Positioning Systems (GPS) [97] for positioning and navigation. A wide-range of applications such as civilian and military navigation, people and asset tracking, emergency rescue and support, mining and exploration, atmospheric studies, smart grids, modern communication systems use GPS for localization and timing. GPS is a satellite-based navigation system that consists of more than 24 satellites orbiting at more than 20,000 km above the earth. Each satellite continuously broadcasts data called *navigation messages* containing its precise time of transmission and the satellite's location. The GPS receiver on the ground receives each of the navigation messages and estimates their time of arrival. Based on the time of transmission that is contained in the navigation message itself and its time of arrival, the receiver computes its distance to each of the visible satellites. Once the receiver acquires the navigation messages from at least four satellites, the GPS receiver estimates its own location and precise time using the standard technique of multilateration.

However, the civilian GPS navigation messages that are transmitted by the satellites lack any form of signal authentication. This is one of the prime reasons GPS is vulnerable to *signal spoofing* attacks. In a GPS spoofing attack, an attacker transmits specially crafted signals identical to those of the satellites but at a higher power that is sufficient enough to overshadow the legitimate satellite signals. The GPS receiver then computes a false location and time based on the stronger spoofing signal transmitted by the attacker. As a result, today, it is possible to spoof a GPS receiver to any arbitrary location. For example, researchers have demonstrated the insecurity of GPS-based navigation by diverting the course of a yacht using spoofed GPS signals [13]. A similar hijack was also successfully executed on a drone using a GPS spoofer that costs less than $1000. More recently, researchers demonstrated a GPS signal generator that can be built for less than $300 [5]. The increasing availability of low-cost radio hardware platforms [3] make it feasible to execute such attacks with less than few hundred dollars worth of hardware equipment. More advanced attacks were demonstrated in [104, 139] in which the attackers *take over* a target receiver that is already locked (continuously receiving navigation messages) onto authentic satellite signals without the receiver noticing any disruption or loss of navigation data. It was shown that a variety of commercial GPS receivers were vulnerable and in some cases even caused permanent damage to the receivers. It is thus evident that these threats are real and it is important to secure GPS from such signal spoofing attacks.

Although spoofing attacks can be, to a certain extent, mitigated by adding cryptographic authentication to the navigation messages (e.g., military GPS systems where the spreading codes are secret), their use requires distribution and management of shared secrets, which makes them impractical for majority of the applications. Even with cryptographic authentication, the system is not protected against relay attacks where an attacker simply records and replays the radio signals to the receiver [106]. Several countermeasures that did not require cryptographic authentication were proposed in recent years either to detect or to mitigate signal spoofing attacks. They rely on detecting anomalies in certain physical characteristics of the signal such as received satellite signal strength, ambient noise floor levels, automatic gain control [19] values and other data that are readily available as *receiver observables* on modern GPS receivers. Some other countermeasures leveraged the signal's spatial characteristics [98, 112] such as the received GPS signal's direction or angle of arrival. All the above-mentioned countermeasures are ineffective against attackers capable of manipulating navigation message contents in real time or a seamless takeover attack [104, 139]. Additionally, the majority of these solutions are not reliable in an environment with strong multipath (signal copies that reach the receiver with a time delay due to reflections in the environment etc.) or in the case of a mobile receiver. Moreover, today there is no receiver platform that can be used to compare and evaluate the effectiveness of these countermeasures in real-world scenarios.

In this chapter, we present a novel GPS receiver which we refer to as SPREE and make the following contributions: SPREE is to the best of our knowledge, the first commercially off the shelf, single-antenna, receiver capable of detecting or significantly limiting all known GPS spoofing attacks described in literature. SPREE does not rely on GPS signal authentication and can, therefore, be used to detect both civilian and military GPS spoofing attacks. Additionally, it is designed to be standalone and does not depend on other hardware such as antennas, additional sensors or alternative sources of location information (like maps or inertial navigation systems). In SPREE, we introduce a novel spoofing detection technique called auxiliary peak tracking that limits even a strong attacker (e.g., seamless takeover) from being able to move (spoof) a receiver to any arbitrary location or time. We leverage the presence of authentic signals in addition to the attacker's signals to detect spoofing attacks. We implement SPREE by modifying an open source software-defined GPS receiver [52] and evaluate it against different signal data sets including the de-facto standard of publicly available repository of GPS signal spoofing traces (Texas Spoofing Battery (TEXBAT) [75]). Furthermore, we evaluate SPREE against COTS GPS simulators and our own traces obtained through an extensive wardriving effort of over 200 km. Our analysis shows that SPREE can reliably detect any manipulations to the navigation message contents. In addition, SPREE severely limits even strong attackers capable of taking over a receiver that is currently locked (receiving and decoding) on to legitimate satellite signals without being noticed. Our evaluations showed that such a strong attacker could offset the SPREE's location to a maximum of 1 km away from its true location. Finally, we release our implementation and a set of recorded GPS signal traces [11] used for evaluating SPREE to the community for further research and development.

6.2 GPS Overview

6.2.1 GPS Satellite System

GPS comprises more than 24 satellites orbiting the earth approximately $20,000$ km above the ground. Each satellite is equipped with high-precision atomic clocks and hence the timing information available across all the satellites are in near-perfect synchronization. Each satellite transmits messages referred to as the *navigation messages* using two frequencies namely 1575.42 MHz (L1) and 1227.60 MHz (L2). The messages are spread using two pseudorandom codes: (i) the coarse-acquisition (C/A) code and (ii) en-

Subframe	Data
1	Satellite clock correction parameters, GPS week
2	Ephemeris data
3	Ephemeris data
4	Almanac data, Ionospheric model, Translation of GPS time to UTC time.
5	Almanac data

Table 6.1: *Contents of the Satellite Navigation Messages*

crypted precision (P(Y)) code. The C/A code is public and contains 1023 bits (also referred to as *chips*) repeated every 1 ms. The P(Y) code is $6.1871 \cdot 10^{12}$ bits long and is repeated once every week at a rate of 10.23 Mbps. The P(Y) code is transmitted using both the L1 and L2 frequency bands and its use is restricted to military and special interest groups. The C/A code is transmitted using the L1 band. In this work, we focus on civilian GPS signals transmitted on the L1 frequency band due to its wide usage in a variety of safety- and security-critical applications.

The navigation data transmitted by each of the satellites consists of a 1500 bit long data frame which is divided into 5 subframes [28]. Subframes 1, 2 and 3 carry the same data across each frame. The data contained in subframes 4 and 5 is split into 25 pages and is transmitted over 25 navigation data frames. The navigation data is transmitted at 50 bps with the duration of each subframe being 6 seconds. Each frame lasts 30 seconds and the entire navigation message, containing 25 such frames, takes 12.5 minutes to be received completely by a receiver.

The data contained in each of the subframes is summarized in Table 6.1. The first subframe mainly contains satellite clock information. The second and third subframes contain the ephemeris i.e., information related to the satellite's orbit and is used in computing the satellite position. Subframes 4 and 5 contain the almanac data i.e., the satellite orbital and clock information with reduced precision. Note that, each satellite transmits the almanac data (subframes 4 and 5) of all other satellites while transmitting only its own ephemeris data (subframes 2 and 3). In the following subsection, we describe the architecture and operation of a typical GPS receiver.

6.2.2 GPS Receiver

Figure 6.1 shows the main components of a GPS receiver. The receiver receives the satellite signals, pre-processes and converts it to digital samples

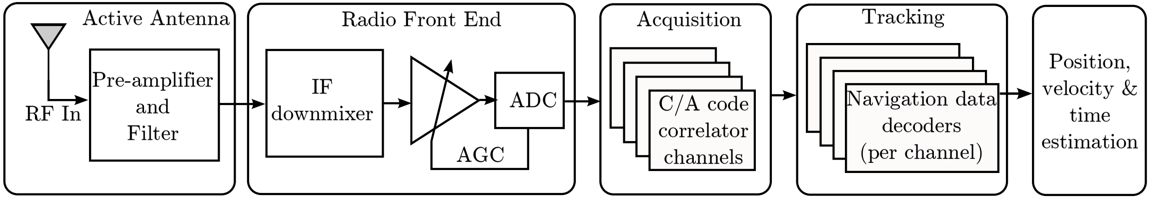

Active Antenna
RF In
Pre-amplifier and Filter
Radio Front End
IF downmixer
AGC
ADC
Acquisition
C/A code correlator channels
Tracking
Navigation data decoders (per channel)
Position, velocity & time estimation

Figure 6.1: *GPS receiver architecture: The satellite signals are received by the receiver's antenna and is pre-processed. The signal is then passed through a automatic gain control (AGC) circuit before it is digitized by the AGC. The receiver then tries to acquire and track satellite signals and if successful it decodes the navigation data and computes a positioning, velocity and time (PVT) solution.*

using an analog-digital converter (ADC). An automatic gain control (AGC) circuit precedes the ADC in-order to monitor and control the power of the ADC's input signal such that it meets the specifications of the ADC. The signal is then forwarded to the acquisition and tracking modules. The acquisition module searches for any available satellite signals. The carrier frequency of a specific satellite signal can differ from its true value due to the relative motion of the satellite and the receiver itself (doppler effect). In addition, the acquisition module needs to determine the pseudorandom code delay of the signal. Thus, in order to detect any visible satellite signal, the receiver performs a two-dimensional search. First, it has to search through all possible delays (phase) of the pseudorandom code. Second, the receiver must account for frequency errors that occur due to doppler effect and other environmental interferences. Thus the receiver's acquisition search for a particular satellite involves scanning for all 1023 possible code delays and doppler frequencies. The receiver accomplishes this by correlating its own replica of the corresponding pseudorandom code with the received signal for each possible satellite. For a stationary receiver, the maximum Doppler frequency shift is around ± 5 KHz and about ± 10 KHz [28] for non-stationary receivers. Assuming a maximum acceptable doppler estimation error of 500 Hz and with 1023 possible code phases to scan, the receiver has to scan through $41,943$ different combinations for each satellite. There are several acquisition strategies such as Parallel Code Phase Search and Parallel Frequency Space Search [28] that parallelize and speedup the acquisition process. If the code and doppler searches result in a correlation peak above a certain threshold the receiver then switches to tracking and demodulating the navigation message data.

Figure 6.2 shows the output of a signal acquisition phase. Typically, GPS receivers have multiple acquisition, tracking and decoding modules to simultaneously search and track different satellites. Commercial receivers are equipped with a number of *channels* (i.e., the number of sets of acquisition, tracking and decoding modules), with each channel searching and tracking one satellite. For example, a 24-channel GPS receiver can simultaneously search for 24 satellites thereby shortening the time to acquire a position fix when compared to a 4-channel receiver. *It is important to note that typical GPS receivers acquire and track only the satellite signal that produces the strongest correlation peak and ignores any weaker correlation peaks as noise.* The decoded data from each acquisition and tracking channel is used to estimate the receiver's range from each of the visible satellites. In order to determine the range, the receiver needs the satellite signal's transmission and reception time. The transmission time of each subframe is found in the navigational message and the reception time is estimated by the receiver. It is important to note

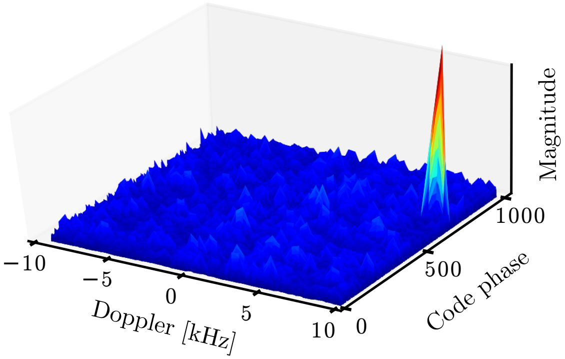


Figure 6.2: *The result of the correlation for a real satellite signal acquisition. As can be seen, there is one strong peak at a certain doppler frequency and code phase.*

that the satellite clocks are in tight synchronization with each other while the receiver's clock (not using atomic crystals) contain errors and biases. Due to the receiver's clock bias, the estimated ranges are referred to as *pseudoranges*. The receiver requires at least four pseudoranges to estimate its position after eliminating the effect of receiver clock bias.

6.3 GPS Spoofing Attacks

A GPS signal spoofing attack is a physical-layer attack in which an attacker transmits specially crafted radio signals that are identical to authentic satellite signals. Civilian GPS is easily vulnerable to signal spoofing attacks. This is due to the lack of any signal authentication and the publicly known spreading codes for each satellite, modulation schemes, and data structure. In a signal spoofing attack, the objective of an attacker may be to force a target receiver to (i) compute a false geographic location, (ii) compute a false time or (iii) disrupt the receiver by transmitting unexpected data. Due to the low power of the legitimate satellite signal at the receiver, the attacker's spoofing signals can trivially overshadow the authentic signals. During a spoofing attack, the GPS receiver locks (acquires and tracks) onto the stronger signal i.e., the attacker's signals, ignoring the legitimate satellite signals. This results in the receiver computing a false position, velocity and time based on the spoofing signals.

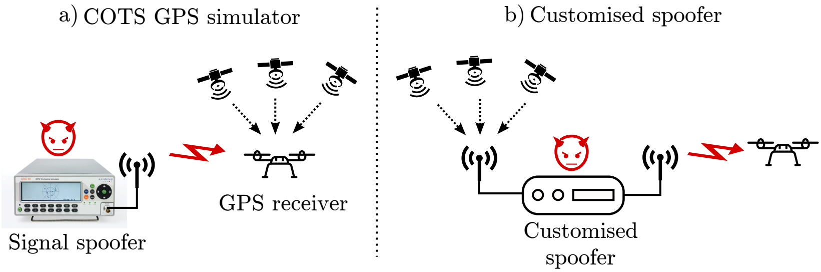


Figure 6.3: *a) Spoofing attack using a COTS GPS signal generator which creates GPS signals from scratch. The generated signals are typically not synchronized with the legitimate satellite signals. b) Spoofing attack with a customized spoofer which can generate 'fake' GPS signals based on the legitimate satellite signals. Depending on the type of the attack, the customized spoofer can be configured to receive authentic GPS signals, modify their navigation messages in real time and replay it to the victim receiver. Such spoofers are capable of creating signals that are code and phase aligned with the authentic signals.*

An attacker can influence the receiver's position and time estimate in two ways: (i) manipulating the contents of the navigation messages (e.g., the location of satellites, navigation message transmission time) and/or (ii) modify the arrival time of the navigation messages. The attacker can manipulate the arriving time by temporally shifting the navigation message signals while transmitting the spoofing signals. We classify the different types of spoofing attacks based on how synchronous (in time) and consistent (with respect to the contents of the navigation messages) the spoofing signals are in comparison to the legitimate GPS signals currently being received at the receiver's true location.

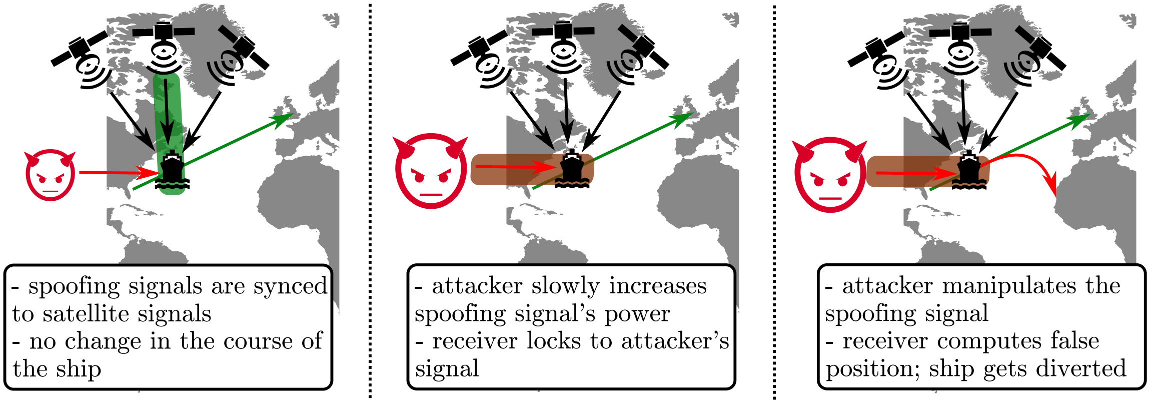
6.3.1 Classification of Spoofing Attacks

Non-Coherent and Modified Message Contents: In this type of an attack, the attacker's signals are both unsynchronized and contain different navigation message data in comparison to the authentic signals. Attackers who use GPS signal generators [4, 6] to execute the spoofing attack typically fall under this category. An attacker with a little know-how can execute a spoofing attack using these simulators due to their low complexity, portability and ease of use. Some advanced GPS signal generators are even capable of recording and replaying signals, however not in real-time. In other words, the attacker uses the simulator to record at one particular time in a given location and later replays it. Since they are replayed at a later time, the attacker's signals are not coherent and contain different navigation message data than the legitimate signals currently being received.

Non-Coherent but Unmodified Message Contents: In this type of attack, the navigation message contents of the transmitted spoofing signals are identical to the legitimate GPS signals currently being received. However, the attacker temporally shifts the spoofing signal thereby manipulating the spoofing signal's time of arrival at the target receiver. For example, attackers capable of real-time record and replay of GPS signals fall under this category as they will have the same navigation contents as that of the legitimate GPS signals, however shifted in time. The location or time offset caused by such an attack on the target receiver depends on the time delay introduced both by the attacker and due to the propagation time of the relayed signal. The attacker can precompute these delays and successfully spoof a receiver to a desired location.

Coherent but Modified Message Contents: The attacker generates spoofing signals that are synchronized to the authentic GPS signals. However, the contents of the navigation messages are not the same as that of the currently seen authentic signals. For example, attacks such as those proposed in [104] can be classified under this category. Nighswander et al. [104] present a Phase-Coherent Signal Synthesizer (PCSS) that is capable of generating a spoofing signal with the same code phase as the legitimate GPS signal that the target receiver is currently locked on to. Additionally, the attacker modifies the contents of the navigation message in real-time (and with minimal delay) and replays it to the target receiver. A variety of commercial GPS receivers were shown to be vulnerable to this attack and in some cases, it even caused permanent damage to the receivers.

Coherent and Unmodified Message Contents: Here, the attacker does not modify the contents of the navigation message and is completely synchronized to the authentic GPS signals. Even though the receiver locks on to the attacker's spoofing signals (due to the higher power), there is no change in the location or time computed by the target receiver. Therefore, this is not an attack in itself but is an important first step in executing the seamless takeover attack.



- spoofing signals are synced to satellite signals
- no change in the course of the ship

- attacker slowly increases spoofing signal's power
- receiver locks to attacker's signal

- attacker manipulates the spoofing signal
- receiver computes false position; ship gets diverted

Figure 6.4: *Seamless takeover attack. The receiver is locked on to the legitimate satellite signals. The spoofing signal is synchronized with the legitimate signal and has the same navigation contents. Next, the attacker slowly increases the power of the spoofing signal. The receiver stops tracking the legitimate signals and locks on to the attacker's signal. Finally, the attacker temporally shifts the spoofing signal causing the receiver to compute a false location and thereby changing the ship's route.*

6.3.2 Seamless Takeover Attack

The seamless takeover attack is considered one of the strongest attacks in literature. In a majority of applications, the target receiver is already locked on to the legitimate GPS satellite signals. The goal of an attacker is to force the receiver to stop tracking the authentic GPS signals and lock onto the spoofing signals without causing any signal disruption or data loss. This is because the target receiver can potentially detect the attack based on the abrupt loss of GPS signal. Consider the example of a ship on its way from the USA to the UK as shown in Figure 6.4. The GPS receiver on the ship is currently locked on to the legitimate satellite signals. In a seamless takeover attack, first, the attacker transmits spoofing signals that are synchronized with the legitimate satellite signals and are at a power level lower than the received satellite signals. The receiver is still locked on to the legitimate satellite signals due to the higher power and hence there is no change in the ship's route. The attacker then gradually increases the power of the spoofing signals until the target receiver stops tracking the authentic signal and locks on to the attacker's spoofing signals. Note that during this takeover, the receiver does not see any loss of lock, in other words, the takeover was seamless. Even though the target receiver is now locked on to the attacker, there is still no change in the route as the spoofing signals are both coherent with the legitimate satellite signals as well as there is no modification to the contents of the navigation message itself. Now, the attacker begins to manipulate the spoofing signal such that the receiver computes a false location and begins to alter its course. The attacker can either slowly introduce a temporal shift from the legitimate signals or directly manipulate the navigation message contents to slowly deviate the course of the ship to a hostile destination. Tippenhauer et al. [139] describe the requirements for an attacker to execute a seamless takeover and move the target receiver towards the intended location.

6.3.3 Proposed Countermeasures

In this section, we discuss existing countermeasures and describe their effectiveness against various types of spoofing attacks. A number of countermeasures were based on detecting anomalies in the physical-layer characteristics of the received signal.

In addition to the estimated position, velocity and time, modern GPS receivers output information pertaining to certain physical-layer characteristics directly as *receiver observables*. Modern GPS receivers can be configured to output, for example, automatic gain control (AGC) values, received signal strength (RSS) from individual satellites, carrier phase values, estimated noise floor levels etc. A number of previous works [19,23,146] proposed using some of the above-mentioned receiver observables to realize spoofing awareness in a GPS receiver. For example, in [146] the authors suggest monitoring the absolute and relative signal strength of the received satellite signals for anomalies, the number of visible satellites (should not be high), simultaneous acquisition of satellite signals, etc. Other countermeasures such as detecting sudden changes to the AGC values were also proposed for detecting GPS spoofing attacks. Automatic Gain Controller (AGC) is a hardware module that varies the gain of the internal amplifier depending on the strength of the received signal. Such countermeasures are at best capable of detecting attackers who transmit their spoofing signal at very high power. They are ineffective against attackers who have better control over their spoofing signal.

Several spoofing detection strategies based on analyzing the distortions present in the output of the receiver's correlation function were proposed in [108, 150]. In an ideal noise-free environment, the correlation output has minimal distortions. The authors argue that during a spoofing attack, the attacker's signal would distort the output of the correlators, which can be used to detect the attack itself. However, the correlation output is also distorted due to multipath signals that arrive a few nanoseconds later than the direct signal. Wesson et al. [150] showed that it is indeed difficult to distinguish between the distortions caused due to a spoofing attack and a legitimate multipath signal. Spoofing detection techniques based on the differences in the inherent spatial characteristics of the received signal such as direction or angle of arrival [34, 98, 111] also face the same challenge of reliably distinguishing between legitimate multipath signals and a spoofing attack. Additionally, they also require additional hardware modifications to the GPS receiver. To summarize, although several countermeasures have been proposed in the literature to detect spoofing attacks, there is no countermeasure today that is effective in detecting strong attackers such as a seamless takeover attack. Moreover, there is no platform that can be used to compare and evaluate the effectiveness of existing countermeasures in real-world scenarios. Today, it is still possible to spoof a victim receiver to any arbitrary location without being detected.

6.4 SPREE – A Spoofing Resistant GPS Receiver

The design of SPREE is largely motivated by the lack of a GPS receiver capable of detecting or constraining all the spoofing attacks known in the literature. In this section, we present the design of SPREE, the first GPS receiver capable of detecting or constraining all known spoofing attacks. Our receiver design consists of two key components: (i) Auxiliary Peak Tracker (APT) and (ii) Navigation Message Inspector (NAVI) module. First, we describe the auxiliary peak tracking module, a novel countermeasure which plays a vital role in constraining even a strong attacker capable of a seamless takeover. The key feature of APT is that it acquires and tracks not only the strongest received satellite signal but also the weaker signals that may be present in the environment. Second, we introduce a navigation message inspector (NAVI) which inspects the decoded contents of the navigation message from every satellite and reports any discrepancies. We show that NAVI is capable of detecting attackers who modify the contents of the navigation message. The Auxiliary Peak Tracker protects SPREE from attackers who are not synchronized (non-coherent) to the legitimate GPS signals currently being received and the Navigation Message Inspector prevents attackers from modifying the contents of the navigation message. The combination of auxiliary peak tracking and the navigation message inspector enables SPREE to reliably detect all types of spoofing attacks.

6.4.1 Auxiliary Peak Tracking (APT)

In this section, we describe the details of our proposed Auxiliary Peak Tracking technique, which is one of SPREE's key features that makes it resilient to spoofing attacks. Typically, GPS receivers have multiple acquisition and tracking modules to simultaneously search and track different satellites. Each set of acquisition and tracking module is called a *channel* and each satellite signal is acquired and tracked by only one channel. For example, a 24-channel GPS receiver can simultaneously search for 24 satellites thereby shortening the time to acquire a position fix when compared to a 4-channel receiver. In other words, the receiver searches for a satellite by allocating each channel to one specific satellite. The receiver acquires or searches for a particular satellite signal by correlating its own replica of that specific satellite's pseudorandom code with the received signal. If the search results in a correlation value above a certain threshold, the receiver then switches to tracking and demodulating the navigation message data. *It is important to note that GPS receivers acquire and track only the satellite signal that produces the strongest correlation peak and ignores any weaker correlation peaks as noise.*

In SPREE, we allocate *more than one* channel to the same satellite. This means that in addition to tracking the signal that results in the strongest correlation, SPREE can also track weaker correlation peaks (if present) for the same satellite. In other words, SPREE does not restrict itself to the satellite signals that produces the maximum correlation, but it also detects and tracks

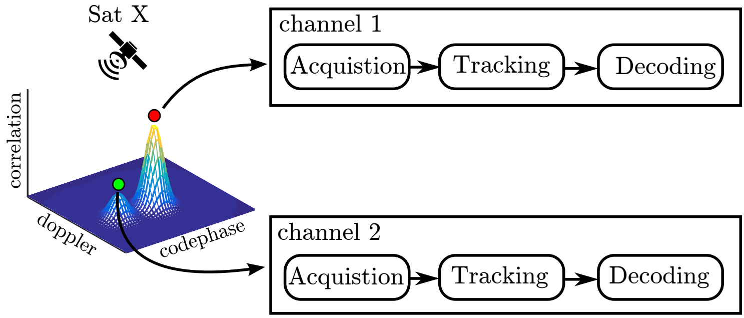


Figure 6.5: *Auxiliary Peak Tracking (APT): SPREE acquires and tracks all multiple signals of the same satellite, even those that produce weaker correlation. In order to track multiple signals, SPREE uses more than 1 channel to acquire, track and decode each satellite's signal.*

signals that produce weaker correlation (Figure 6.5).

Spoofing detection by tracking auxiliary peaks: The Auxiliary Peak Tracker protects SPREE from attackers who are not synchronized to the authentic GPS signals. Recall that the attacker transmits spoofing signals with a higher power such that the authentic GPS signals are overshadowed. Even though the spoofing signals have successfully overshadowed the authentic signals, they are still present in the environment and it is difficult for an attacker to completely annihilate them. In order to completely annihilate authentic GPS signals, the attacker first needs to know the precise location (cm level) of the receiver. Furthermore, he needs to annihilate all the multipath components of the GPS signal at the receiver. This means that the attacker should be able to transmit nulling signals such that they cancel both the direct GPS signal and *all* the possible multipath components at the receiver. In case the receiver is in motion, the attacker must be able to predict the *exact* trajectory of the receiver.

Given the difficulty of completely annihilating authentic satellite signals, they will appear as auxiliary peaks when the attacker's spoofing signals are non-coherent or in other words not synchronized with the authentic satellite signals. We provide a more detailed analysis on how SPREE's APT module enables detection of even the strong seamless takeover attackers in Section 6.6.

6.4.2 Navigation Message Inspector (NAVI)

The Navigation Message Inspector module inspects the decoded navigation data for consistency and sanity and is key to protecting the GPS receiver from

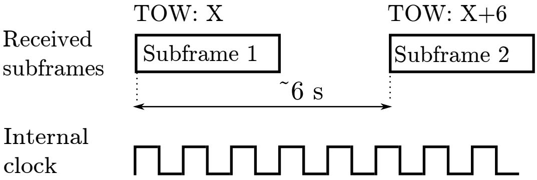


Figure 6.6: *SPREE compares the received TOW to its internal clock to validate that the TOW is increased only in 6 s intervals.*

attackers who modify the contents of the navigation message.

Time of Week (TOW) and Receiver's Clock: One of the key parameters that an attacker can modify in order to spoof a target receiver's location or time is the transmission time of the navigation messages. The navigation data transmitted by each of the satellites are divided into 5 subframes. Each subframe begins with a handover word which contains a truncated version of the time of week (TOW) at which the satellite transmitted that particular subframe. Each subframe lasts for about 6 seconds and since the TOW is transmitted once every subframe, it can only increase in steps of 6 seconds. We leverage the internal clock of SPREE's hardware and the fact that the TOW can only change in steps of 6 s to detect spoofing attacks (Figure 6.6). SPREE records the received GPS week and time of week with its internal clock count and raises an alarm if the difference in the time elapsed internally doesn't match the newly received GPS time of week.

Satellite Orbital Positions: In addition to the transmission time of the navigation message, an attacker can also modify the satellite's position in the orbit. The GPS receiver estimates the satellite's position from the ephemeris data. For example, Nighswander et al [104] demonstrated that it is possible to modify the ephemeris data such that the receiver estimates the satellite to be in the middle of the earth. The authors executed such an attack by setting the square root of the semi-major axis of the satellite's orbit to 0. In our design, an attacker cannot execute such manipulations as SPREE continuously monitors and evaluates any changes to the orbital parameters.

Almanac & Ephemeris Data: SPREE continuously monitors the decoded navigation data from all the visible satellites and performs a number of consistency checks. The almanac and ionospheric model data should be the same across all the navigation frames received from all the satellites. In addition, whenever feasible SPREE leverages the availability of navigation data such as ephemeris, almanac and the ionospheric models from third-party sources to compare the data decoded by the GPS receiver. This data is then compared against the information received from the satellites and is used to detect spoofing attacks.

Thus, SPREE's navigation message inspector independently protects the receiver from attackers capable of modifying the navigation message. By combining the NAVI and APT modules, SPREE detects or constraints all types of attacks capable of spoofing the receiver's location and time.

6.5 Implementation

We implemented SPREE based on GNSS-SDR [52], an open source software-defined GPS receiver. GNSS-SDR is written in C++ and can be configured to process signals received directly from a radio hardware platform such as USRP [3] or from a file source. GNSS-SDR works with a range of hardware platforms and signal recorders such as USRP, SiGe GN3S Sampler, NSL Primo [9], IFEN's NavPort [12] etc. The architecture of GNSS-SDR largely resembles the design of a typical GPS receiver as described in Section 6.2. It consists of a signal source and a conditioner module which are responsible for interfacing with the underlying receiver hardware or file source. Similar to typical GPS receivers, GNSS-SDR also consists of several *channels*; each individual channel managing all the signal processing related to a single satellite. In GNSS-SDR, the *channel* is a software module that encapsulates the functions of acquisition, tracking and navigation message decoding blocks. All the channels then report to a module that estimates the pseudoranges and a number of other observables. Finally, if enough information is available, the receiver calculates a position, velocity, and time. A configuration file allows the user to chose operational parameters such as the sampling frequency, the algorithms to use for each processing block, signal source etc. We modified the acquisition and tracking modules of GNSS-SDR to realize SPREE. First, we implement the auxiliary peak tracking system within the GPS receiver's acquisition module. Recall that the auxiliary peak tracker enables the receiver to track multiple signals of the same satellite instead of limiting it to the strongest component only. We implement the navigation message inspector which checks the consistency and sanity of the extracted navigation data within the tracking module of the receiver.

Auxiliary Peak Tracking (APT): In SPREE, when a particular satellite is assigned to a channel, all local peaks of the acquisition correlation function, which are above a certain threshold are collected and stored for processing. This is in contrast to the modern receivers only choosing the highest correlation peak. Each local peak is then assigned to a different channel in descending order of magnitude for tracking. The maximum number of channels that can track the same satellite is made configurable at run time. The number of channels that can be assigned to track the same satellite will influence the number of peaks that can be evaluated at the same time.

If SPREE is successful in acquiring more than one peak, it records the differences in their arrival times i.e., the separation between two peaks. If the difference is more than the maximum acceptable time difference, τ_{max}, SPREE detects a spoofing attack. The value τ_{max} is set in the configuration file. This check is done each time a new navigational message is received. The arrival time is computed by the tracking module, where it is estimated based on the sample counter of GNSS-SDR and fine tuned based on the code phase of the satellite signal. After an auxiliary peak has been acquired, tracked and evaluated for signs of spoofing and none are found it is dropped and the channel is free to acquire another auxiliary peak to evaluate. If the peak remains it will be evaluated again when a channel is free *and* all other peaks have been evaluated.

Navigation Message Inspector (NAVI): In GNSS-SDR, a telemetry decoder is responsible for decoding the contents of the received navigational message. First, SPREE records the time of week decoded from each of the received navigation message subframes. If the difference in time of week present in consecutive subframes does not match with its internal clock count (more than 6 s difference due to the minimum resolution), SPREE raises an alarm. Next, the stored navigation data for each of the visible satellites is compared with the contents of the preceding navigation message for that particular satellite. If there is a discrepancy between these two values, SPREE notes it as a possible spoofing attack. Also, SPREE compares the navigational data from all satellites with each other for any discrepancies in the almanac and ephemeris data. Recall that, the almanac and ionospheric model data should be the same across all the navigation frames received from all the satellites. If configured to do so and if possible, it can also compare the time, almanac, ephemeris and the ionospheric model data received from the satellites to data received from third-party sources using the Secure User Plane Location (SUPL) protocol. These checks are done each time a new navigation message is received.

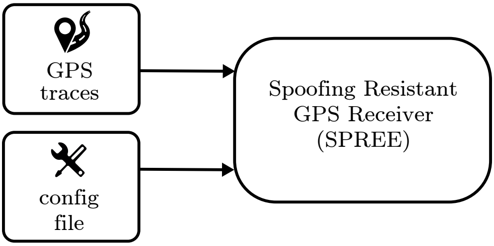


Figure 6.7: *Evaluation Setup: A configuration file specified vital system parameters such as input source, source signal sampling rate and configuration of the spoofing detection module.*

In addition to the above modules, we also implement several existing countermeasures described in Section 6.3 to facilitate real-world performance evaluations. However, we restrict our discussion to our main contributions, the APT and NAVI module as they enable reliable detection of all known spoofing attacks in literature. It is important to note that SPREE adds no additional requirements on the underlying hardware and supports all the platform and file sources supported by GNSS-SDR. It is possible to toggle any of SPREE's spoofing countermeasures in the configuration file as shown in Table 6.2.

6.6 Security Evaluation

In this section, we evaluate SPREE and present its security guarantees. Figure 6.7 shows our evaluation setup. A configuration file is used to select SPREE's parameters including those needed by the spoofing detection module. In our evaluations, the GPS signal traces (spoofing and clean) were recorded and stored in files and later input to SPREE. We evaluated SPREE against three different sets of GPS signals: (i) a public repository of spoofing traces (TEXBAT) [75], (ii) signals recorded through our own wardriving effort and (iii) spoofing signals generated using COTS GPS simulators.

6.6.1 GPS Traces

GPS Simulator: First, we evaluated the performance of SPREE against our own spoofing signals generated using commercially available GPS simulators. Specifically, we used Spectracom's GSG-5 Series advanced GPS simulator [4] in order to generate our spoofing signals. One of the key features of the simulator is its ability to generate multipath signals for any satellite. It is even

Parameter	**Description**
ap_detection	Enables or disables auxiliary peak spoofing detection block (default=true)
nr_acquisitions	Maximum number of channels allocated for each satellite
max_rx_discrepancy	Maximum acceptable difference in time-of-arrival (in seconds) between signals from the same satellite
alt_detection	Enables or disables evaluation of the height of the calculated position
alt_max	Maximum expected height.
inter_satellite_detection	Enables or disables navigational data consistency check between satellites.
external_nav_check	Enables or disables navigational data consistency check against 3rd party sources.
external_source	Specifies source of 3rd party navigational data, can either be a file or SUPL server. GNSS-SDR already allows a user to specify a SUPL server so these configurations are used if this option is chosen.

Table 6.2: *Sample set of SPREE's parameters that can be configured during run time within the config file.*

Trace	Scenario	Synchronization	Type	Power Adv
Tr_{ssw}	Static	N/A	None	N/A
Tr_{smp}	Static	Frequency lock mode	Position	0.4
Tr_{smt}	Static	Frequency lock mode	Time	1.3
Tr_{sot}	Static	Code Phase Proportional	Time	10
Tr_{sca}	Static	Carrier Phase Aligned	Time	Matched†
Tr_{scer}	Static	Carrier Phase Aligned	Time	Matched†
Tr_{dmp}	Dynamic	Frequency lock mode	Position	0.8
Tr_{dot}	Dynamic	Code Phase Proportional	Time	9.9

Table 6.3: *Summary of the TEXBAT GPS Spoofing Traces. Code Phase Proportional means that the counterfeit signals' carrier phase is proportional to the code phase change. Frequency Lock mode indicates that the initial phase offset between the counterfeit signals and the authentic signals is maintained throughout the spoofing scenario. † The spoofing signals are power matched but precise values are unknown.*

possible to configure the multipath's power levels and time offset i.e., the extra distance traveled by the multipath relative to the original line-of-sight (LOS) signal. The GPS simulator traces were mainly used to evaluate the ability of SPREE to robustly detect auxiliary peaks. In addition, we used the GPS simulator traces to simulate attackers capable of manipulating the content of the navigation messages.

Texas Spoofing Test Battery (TEXBAT): TEXBAT [75] is a set of digital recordings containing both static and dynamic civilian GPS spoofing tests conducted by the University of Texas at Austin. TEXBAT is the only publicly available dataset and the de-facto standard for testing spoofing resilience of GPS receivers. TEXBAT includes two clean data sets, one each for a static and dynamic receiver setting, in addition to eight spoofing scenarios based on the location and time of the clean GPS traces. The properties of the spoofing scenarios are summarized in Table 6.3. The static switch scenario (Tr_{ssw}) replicates the case where the attacker has physical access to the target's antenna and can thus completely remove the authentic signals and replace them with his counterfeit signals. All other scenarios perform a take-over attack where either the time or position of the target receiver is spoofed. TEXBAT also includes a scenario (Tr_{scer}) where a security code estimation and replay (SCER) attack [74] is performed. In an SCER attack, the attacker attempts to guess the value of the navigational data bit in real time. The spoofing signals

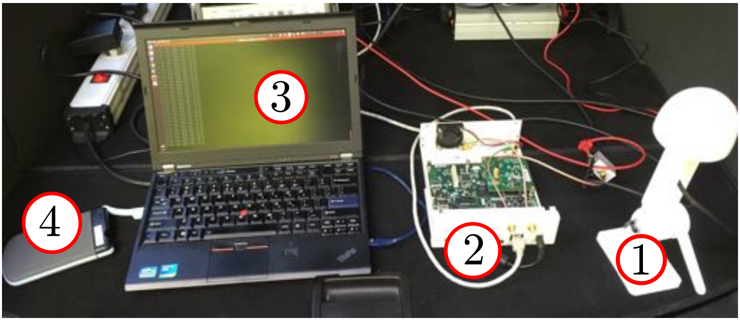


Figure 6.8: *Our wardriving setup with a front-end consisting of a (1) a active conical GPS antenna and a (2) USRP N210. The signals were recorded using a (3) laptop. The recordings were periodically moved to an (4) external hard disk.*

are closely code-phase aligned with the authentic signals. However, the carrier phase alignment of the spoofing signals with the authentic signals depends on the scenario. For example, when the attacker attempts to spoof the victim receiver's position or time, the carrier phase is manipulated such that the rate of change of spoofing signal's carrier phase equals that of the authentic signal. In two spoofing scenarios (Tr_{sca} and Tr_{scer}), the carrier phase of the spoofing signal is also aligned to the authentic GPS signals during the take over. In remaining scenarios, the attacker's signals' carrier phase is either proportional to the code phase change (Code Phase Proportional) or the initial phase offset between the counterfeit signals and the authentic signals is maintained throughout the spoofing scenario (Frequency Lock mode).

Wardriving: In addition to using TEXBAT scenarios, we collected our own GPS traces through an extensive wardriving effort. We used the wardriving dataset to evaluate SPREE's behavior in a non-adversarial (only legitimate GPS signals present) scenario and determine how reliable is SPREE with respect to false alarms. The setup used for recording the GPS signals during the wardriving effort is shown in 6.8. The front end of the setup consists of an active conical GPS antenna and a bias-tee. We used a USRP N210 and GNURadio and recorded raw GPS signals into an external hard disk. The signals were sampled at 10 MHz and stored in complex data format. The setup itself was powered through the car's power outlet. We recorded the GPS signals at various locations: (i) An open field, (ii) parking lot of a small

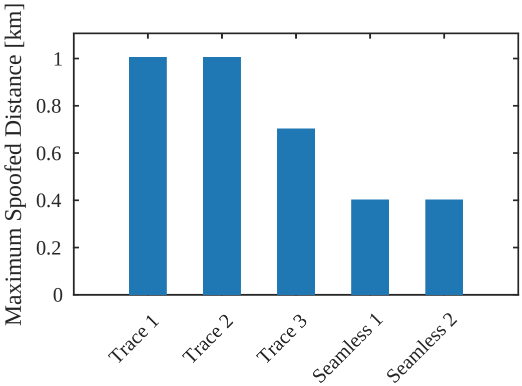


Figure 6.9: *Spoofing detection in TEXBAT dataset. SPREE detected auxiliary peaks in all the spoofing traces. The maximum location offset the attacker could cause before being detected was less than a kilometer.*

village, (iii) driving on a highway, (iv) driving inside a city, (v) inside a city with neighbouring tall buildings and (vi) inside a forest with dense tree cover.

6.6.2 Security Evaluation

Recall that an attacker can influence the receiver's estimates by either manipulating the contents of the navigation messages or temporally shifting the navigation message signals while transmitting the spoofing signals.

Detecting Non-coherent Attackers: Recall that a non-coherent attacker's spoofing signal is not synchronized with the authentic satellite signals. Even though the receiver might be locked on to the attacker's spoofing signals, the authentic signals will appear as auxiliary peaks due to the Auxiliary Peak Tracking module. The effectiveness of detecting such non-coherent spoofing attacks depends on the ability of the APT module to detect and track auxiliary peaks. First, using our own GPS simulator traces, we tested the ability of the APT module to detect and track multiple acquisition correlation peaks. Specifically, we leveraged the ability of the simulator to generate duplicate copies of a satellite signal at different time intervals away from the original signal. We generated signal copies spaced between 50 ns to 1000 ns and determined that our receiver was able to reliably detect and track auxiliary peaks spaced 500 ns or more. In some scenarios, it was able to track peaks much closer, however not reliably (over multiple runs). Thus, we configured APT module to track auxiliary peaks that are separated by more than 500 ns.

The choice of 500 ns separation between two peaks for spoofing detection is supported by two additional reasons: (i) During signal acquisition (searching for satellite signals), GPS receivers shift their correlator typically by half a chip[1] period i.e., 500 ns. This means that most modern receivers can reliably track peaks that are separated by 500 ns and no additional hardware changes are required to implement SPREE in modern receivers. (ii) Several prior works on modeling GNSS multipath signals [32, 84, 88, 93] show that most GPS multipaths are delayed by less than $300-400$ ns. This means that it is highly unlikely to observe an auxiliary peak caused due to legitimate multipath signals occurring at more than 500 ns away from the line-of-sight signal peak. Moreover, the attenuation and polarization shift introduced in the legitimate signals due to reflections that are a few hundred meters away would make the signal untrackable. We proceeded to evaluate SPREE against the TEXBAT set of GPS spoofing signal traces described previously. SPREE detected auxiliary peaks in all the traces containing spoofing signals and failed to detect any auxiliary peaks for the clean non-spoofing traces. Based on the separation of auxiliary peaks at the time of detection, we evaluated the maximum possible location offset an attacker could have caused without being detected and present it in Figure 6.9. In the case of the seamless takeover attacks, the maximum deviation an attacker could introduce in SPREE was about 400 m. It is important to note that traces 1, 2 and 3 contain spoofing signals that are not as closely synced as the seamless takeover traces and hence the larger values for maximum spoofed distance. For completeness, we processed our wardriving traces that represent clean, non-spoofing scenarios for any false alarms. SPREE did not detect any auxiliary peaks.

Detecting Navigation Message Modifications: We will now analyze SPREE's resilience against attackers who modify the contents of the navigation message. The key parameters that an attacker can manipulate the navigation data are the time of transmission and the satellite's orbital information present in the almanac and ephemeris.

Modifying TOW: As described in Section 6.4.2, the value of TOW can be altered only in steps of 6 seconds. SPREE leverages the internal clock of the hardware receiver to continuously compare the received TOW data against its internal clock count. SPREE raises an alarm if the difference in the time elapsed internally doesn't match the newly received GPS time of week information. We note that even a watch crystal today has an error rating of

[1] A chip is one bit of the pseudorandom code

approximately 10 ppm which is a drift of less than a second in one day. Therefore a drift of 6 s can be easily detected even without a thermally controlled crystal oscillators (TCXO[2]) that are present in modern hardware receiver platforms. We evaluated SPREE against such an attack using two GPS simulators each spoofing the same satellite however with different TOW data and SPREE successfully detected the attack. Both the simulators were synchronized to the same reference clock signal. We used this setup to evaluate SPREE's resilience to attacks described in [104] such as arbitrary manipulation of week numbers and date desynchronization attacks.

Modifying Ephemeris Data: The attacker can also manipulate the ephemeris data to force the receiver to malfunction. Ephemeris data gets updated once every two hours and contain precise satellite orbital information including satellite clock biases. However, it was shown in [104] that it is trivial to force a receiver to accept ephemeris changes whenever possible. Since SPREE's NAVI module keeps track of the elapsed time using the receiver's internal clock, it can be configured to ignore any ephemeris updates within the 2-hour time interval. It is also important to note that any changes to the satellite orbital information or in general the ephemeris data can be compared against ephemeris data available from third-party sources [8]. Additionally, SPREE is capable of recording the ephemeris data received from all satellites in the past and notify if there is any unexpected change in the ephemeris data values.

Detecting Seamless Takeover Attack: As described previously, a seamless takeover attack is an attack in which the attacker takes control of the victim receiver without any disruption to its current state. This type of attacker is one of the strongest attackers known in the literature and no existing countermeasure is effective in detecting the seamless takeover attack. We will now see how SPREE enables detecting a seamless takeover attack. Consider the same example of a ship on its way from the United States to the UK, currently locked on to legitimate satellite signals. The attacker begins a seamless takeover by transmitting spoofing signals that are synced to the legitimate satellite signals but at a lower power level. The output of the acquisition module is shown in Figure 6.10. Notice that the legitimate satellite signal (shown in green) is stronger than the spoofing signal but are synchronized to each other. Now the attacker increases the spoofing signal's power and takes over the receiver. Note that, even though the receiver is locked on to the attacker, there is still no change in route yet. This is because the attacker is both synchronized to the

[2] Modern TCXOs have error ratings between $1-100$ ppb and are available for under $10

legitimate signals and is transmitting the same navigation message. Now, the attacker begins to drift the spoofing signal away with the intention of changing the course of the ship. At this point, a typical GPS receiver will ignore any weaker correlation peaks that exist and compute its location based on the attacker's signal. However, SPREE will detect an auxiliary peak and rise an alarm.

Maximum position offset: Recall that, SPREE detects any modifications to the contents of the navigation message and tracks peaks of the same satellite that are separated by more than 500 ns. This value was setup after extensive experiments using signals from GPS simulators and our own wardriving efforts as described previously. This means that the attacker is limited to temporally shifting his spoofing signals by at most 500 ns which result in a 150 m change in the pseudorange estimated by the receiver for that specific satellite. It is important to note that the effect of this change in pseudorange caused by the attacker on the receiver's final position estimate depends on the constellation of the satellites. We collected all the different constellations observed during our wardriving and evaluated the effect of temporally shifting the satellite pseudoranges by 150 m. Our analysis accounted for all possible pseudorange changes an attacker can introduce on all combinations of visible satellites. We analyzed over 73 different satellite constellations, each one with four satellites, and calculated the maximum possible location offset an attacker could introduce. Our results are shown in Figure 6.11. On an average the maximum position deviation was 455 m. This means that e.g., in the ship hijack scenario, it would not be possible for an attacker to deviate the course of the ship by more than 455 m. Note that, we limited our analysis to constellations consisting of only four visible satellites, which is the most favorable for an attacker. In most environments, more than four satellites will be visible, which will further constrain how much the attacker can change the victim's position. Furthermore, we observed that the constellations that allow the attacker to spoof the receiver more than 1 km away, comprised satellites at very low elevation angles. Therefore, configuring SPREE to only accept satellite signals with a minimum elevation angle will potentially constrain the attacker further.

6.7 Discussion

Integrating SPREE into commercial receivers: One of the main differences between SPREE and a commercial GPS receiver is that unlike commercial

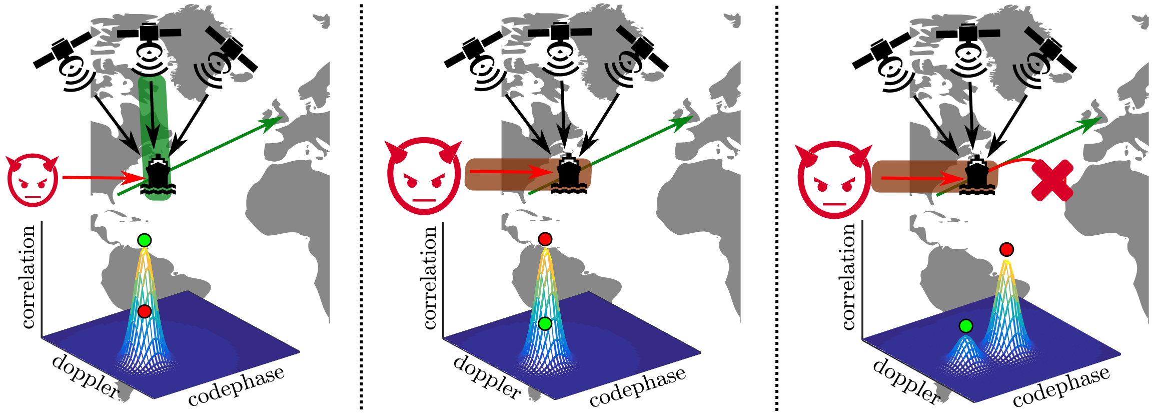


Figure 6.10: *Detecting seamless take over attack. As the attacker begins to drift the spoofing signal away with the intention of changing the course of the ship, SPREE will detect the auxiliary peak produced by the legitimate satellite signal and rise an alarm.*

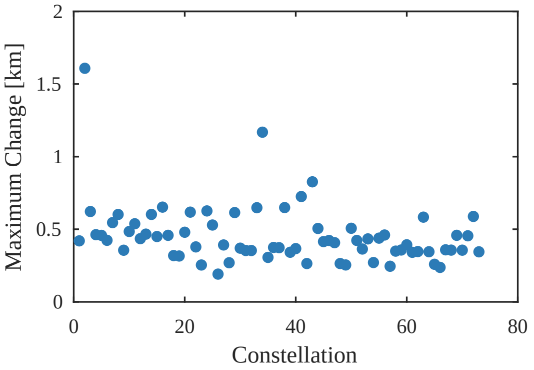


Figure 6.11: *Maximum location offset. An analysis of 73 satellite constellations (as observed during wardriving) show that a strong attacker can cause a maximum location offset of less than 1 km in majority of the scenarios before being detected.*

receivers which track one satellite per channel, SPREE uses multiple channels to track the same satellite. This means that without any hardware changes i.e., for the same number of acquisition and tracking channels, our spoofing-aware receiver will track less number of satellites than its capable of. In order to do this, two changes are necessary: (i) allocate a minimum of two channels for every visible satellite signal (one for the authentic GPS signal and one that keeps searching for a potential spoofing signal) and (ii) search the entire range of time delays for weaker acquisition peaks. The number of channels allocated per visible satellite signal can be easily modified in the firmware. However, as mentioned before, this will limit the number of satellites that the receiver can simultaneously acquire and track. Modern receivers typically have $32-128$ channels capable of tracking $32-128$ satellites simultaneously[3] and allocating two channels for each satellite will reduce the number of satellites that can be tracked by half. In reality, this is not a problem since the typical number of visible satellites at any time instant is not more than 10 or 11. In order to track auxiliary peaks, we keep a list of all auxiliary peaks found during the acquisition in a float array. The number of floats stored is $2 \cdot \frac{F_s}{1000}$ for each acquisition, where F_s denotes the sampling rate. This means that for a sampling rate of 10 MHz each acquisition requires an additional $\approx 19.5\,\text{kB}$ of

[3] sometimes used in receiver's capable of using more than one satellite navigation system such as GLONASS

storage. We believe this to be negligible when compared to the available RAM in most of the modern receivers today. There is practically no performance overhead in detecting changes to the contents of the navigation message by an attacker. The only waiting time is the time (≈ 6 s) needed to receive and decode the new subframe completely. Hence, our design modifications can be easily integrated into a modern GPS receiver with only a firmware upgrade and does not require any changes to the underlying hardware.

Probability of False Alarms: False alarms can be caused due to an event that forced SPREE to believe it is being spoofed. In the case of the auxiliary peak tracking module, the arrival of a legitimate multipath signal with a delay of more than 500 ns and with a signal strength greater than the acquisition threshold will result in SPREE raising a spoofing alert. This is unlikely to be captured by the GPS receiver due to the following reasons: (i) change in polarization–GPS signals are typically right-hand polarized and any reflections causes a change in the polarization of the signal. The majority of GPS receiver antennas are configured to received the direct right hand circularly polarized signals and attenuate reflected signals. (ii) Propagation path loss–Since the multipath signals travel a few hundred meters more than the direct line of sight signal, the signals undergo more attenuation due to propagation path loss. Also, reflections from surfaces themselves may cause the GPS signal to attenuate and therefore, given the received power levels of the direct line of sight GPS signals on the ground, multiple reflections would eventually only make the signal untrackable. In addition, auxiliary peaks caused by legitimate multipaths tend to be momentary and untrackable in contrast to a peak caused by a seamless takeover attack. Recall that, SPREE did not detect any auxiliary peak beyond the set τ_{max} of 500 ns on the traces collected during our wardriving effort. In fact, an analysis of the temporal behavior of multipath signals against spoofing signals can enable distinct identification of peaks caused due to a spoofing signal. Note that, even after detecting auxiliary peaks, it is currently difficult to distinctly identify the peak caused by the spoofing signal and that caused by the legitimate signal. Thus, the results of the temporal behavioral analysis can help the receiver to ignore or internally cancel the spoofing signal and thereby building better resilience to spoofing attacks.

Limitations: One of the limitations of SPREE is it is only capable of detecting a spoofing attack. Even though detecting all known spoofing attacks is a significant improvement over the state of the art, the ability to annihilate or neutralize the attacker's spoofing signal will enable the receiver to continue operation even in the scenario of an attack. In the case of SPREE, the significant challenge in canceling the spoofing signal is the ability to determine the source of the auxiliary peak. For example, SPREE will raise an alarm once it detects an auxiliary peak. However, SPREE is incapable of identifying the exact peak that is caused by the attacker's spoofing signal.

6.8 Related Work

The work that comes closest to SPREE is the design of an inline anti-spoofing device [86]. The device connects between the GPS antenna and a GPS receiver and uses complex correlation peak distortion techniques to identify spoofing signals. As demonstrated in [150], such countermeasures face the challenge of distinguishing spoofing signals from real-world channel effects and are ineffective against seamless takeover attackers. Also, the device is incapable of detecting attackers who modify the contents of the navigation messages.

Several works [53, 80, 85, 92, 149, 151] propose solutions that are cryptographic in nature and therefore require modifications to the GPS infrastructure. Incorporating cryptographic authentication into civilian GPS, similar to military GPS, could to an extent mitigate spoofing attacks. However, this would require distribution and management of shared secrets which makes it infeasible for a large set of applications. Additionally, cryptographic authentication does not protect against signal replay attacks where an attacker simply records legitimate GPS signals at one location and replays it to the victim receiver [106].

Another set of spoofing detection techniques were based on the differences in the inherent spatial characteristics of the received signal such as direction or angle of arrival. In order to measure these spatial characteristics, multiple antennas or movement of a single antenna is required. These works additionally assume that the attacker uses a single antenna or spoofer to transmit the spoofing signal. In [98], the authors measure carrier phase values using a dual antenna array. With the knowledge of orbital information of a satellite, it is possible to theoretically estimate the expected carrier phase measurements for each satellite at the receiver. Spoofing is detected by comparing the theoretical carrier phase estimates against observed carrier phase measurements. Psiaki et al. [112] eliminated the need for multiple antennas by setting the receiver antenna in small random motions. In a spoofing attack, the observed carrier phase values of all the spoofed satellite signals will exhibit variation identical to the antenna motion. In a non-adversarial setting, the carrier phase values will vary independently due to the physical separation of satellites in space. Several similar techniques proposed in the literature are surveyed in [79]. All the above works require additional hardware modifications to existing GPS receivers. For example, [98] requires an additional antenna and signal processing circuits while [112] requires high-frequency carrier phase estimates–none of those are available in currently available GPS receivers. Another approach to solving the multiple antenna requirement was proposed in [34]. The authors monitor the amplitude and doppler correlation of visible satellite signals by moving an antenna along a *predetermined trajectory*. The above countermeasures are ineffective in real-world scenarios, especially in the presence of multipath signals. For example, GPS signals reflected from buildings or moving objects would appear to be spoofing signals and therefore cause false alarms. Additionally, if an attacker uses drones flying overhead to transmit the spoofing signals, their angle of arrival would not appear to be abnormal.

Some other proposals depended on additional hardware such as additional receivers, alternative navigation systems, sensors etc. Tippenhauer et al. [139] proposed the use of multiple synchronized GPS receivers to detect spoofing. They show that spoofing a set of synchronized GPS receivers, with known relative distances or geometrical constellation restricts the number of locations from where an attacker can transmit the spoofing signals. Cross-validation of the position estimates against alternate navigation systems such as Galileo [73] were also proposed. However, a simulator that can spoof both GPS and Galileo will easily defeat this countermeasure. Data from other sensors can also be used to cross validate GPS navigation solutions. For example, inertial measurement units (e.g., accelerometer, gyroscope, compass) have already been proposed as alternative ways to navigate during temporary GPS outages [51, 140, 148]. The main drawback of inertial navigation units is the accumulating error of the sensor measurements. These accumulated sensor measurement errors affect the estimated position and velocity over a longer duration of time and hence limit the maximum time an IMU can act independently.

6.9 Conclusion

In this chapter, we presented SPREE, the first GPS receiver that detects all known spoofing attacks. We designed, implemented and evaluated SPREE against different sets of signal traces and showed that even a strong attacker capable of a seamless takeover cannot deviate the receiver by more than 1 km. This is a vast improvement over current GPS receivers that can be spoofed to any arbitrary location in the world. Finally, we release our implementation and the GPS dataset used in our evaluations to the research community.

Chapter 7

Closing Remarks

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.

7.1 Summary

We began this thesis by illustrating the rise of new applications that depend on location and proximity and the need to ensure their security against modern day cyber-physical attacks. We summarized the state of the art in the field of secure proximity verification in Chapter 2 and enumerated their advantages and limitations. We showed that there is still a lot of scope for improving the state of the art with respect to the actual realization of these systems. Existing systems either did not protect against all known distance modification attacks or were unsuitable for applications such as contactless payments that require the prover's hardware to be fully passive.

In Chapter 3, we proposed *Switched Challenge Reflector with Carrier Shifting*, a hybrid digital-analog design that enabled the realization of efficient Terrorist Fraud resilient systems. Until now, in the space of distance bounding protocol implementations, we could either build efficient implementations, that resist Distance Fraud and Mafia Fraud but not Terrorist Fraud attacks, or less efficient implementations that resist all three types of attacks. Furthermore, we introduced a novel attack called the double read-out attack and showed how our design also protects against this attack.

In Chapter 4, we analyzed the security of chirp-based ranging systems as chirp signals enable designing low-complexity, power efficient ranging systems. We showed that chirp-based ranging systems as they are in use today are vulnerable to physical-layer relay attacks namely early detect and late commit. Specifically, we demonstrated that an attacker can impersonate an honest prover and claim to be within a meter of the verifier even though the legitimate prover is as far as 700 m away from the verifier.

In Chapter 5, we proposed a secure proximity verification system design with a ranging precision and security guarantees that make it suitable for contactless access control and authentication applications. We leveraged backscatter communication to enable the realization of fully-passive or semi-passive provers. We also demonstrated how our proposed system protects against conventional distance modification attacks. Furthermore, even a strong attacker capable of executing early detect and late commit attacks can introduce a distance ambiguity of not more than a meter. The proposed design carefully considered the security vulnerability findings chirp-based ranging systems presented in Chapter 4.

Finally, in Chapter 6 we presented SPREE, the first GPS receiver (at the time of writing this thesis) capable of detecting or mitigating all GPS spoofing attacks described in the literature. SPREE used a novel spoofing detecting technique based on auxiliary peak tracking that constrained even an attacker capable of seamlessly taking over a GPS receiver that is locked on to legitimate satellite signals. The seamless takeover attack is considered the strongest attacker in the literature. SPREE was implemented and evaluated against different sets of spoofing and non-spoofing (clean) scenarios and demonstrated how SPREE is resilient to spoofing attacks.

7.2 Future Work

In this section, we provide insights for future work in the field of secure localization and proximity verification with the end goal of designing and deploying a wide-area secure localization and proximity verification system.

Improving Evaluation of Physical-layer Attacks: It is clear from this thesis that physical-layer attacks on ranging systems are highly time-constrained. For example, as seen in Chapters 5 and 4, in order to effectively execute an early detect and late commit attack on a ranging system, the attacker must be able to predict the symbol within a few nanoseconds. Even in the case of a seamless takeover attack on modern GPS receivers (Chapter 6), the attacker must be synchronized precisely with that of the legitimate satellite signals. Existing radio platforms such as USRP have a processing delay of the order of few microseconds before the received signal is decoded; which makes them unsuitable without modification for implementing ED and LC attacks. Therefore, it is essential to realize an end-to-end hardware module with small processing delay and capable of executing physical-layer attacks such as ED, LC in real-time. Such a platform would enable security analysis of the proposed secure localization and proximity verification solutions against strong attackers.

Prototyping the Passive Prover Design: As part of future work, we intend to build a complete prototype to fully evaluate our proposed FMCW-based secure proximity verification system. The work presented in Chapter 5 is a first step towards realizing a distance bounding system in which the prover can be fully passive. We evaluated our proposed design using an experimental setup, however, what was lacking is the real implementation of a contactless card with the complete system integrated. Such an implementation is important for real-world deployment and can potentially give rise to interesting implementation challenges that were not previously discovered.

In addition, the feasibility of using other modulation methods e.g., phase-shift keying (PSK) over FMCW remains to be explored. The nominal values for the security-relevant parameters such as the time required to early detect and late commit under these modulation schemes also needs to be investigated further. For example, using chirps signals for ranging and a m-ary PSK scheme (i.e., encoding data in the phase transitions between symbol periods) for data modulation will potentially reduce the time window available to the attacker for executing an early detect and late commit attack. Therefore, the possibility of distance decreasing attacks would depend on the particular synchronization and decoding procedures which need to be further explored.

Enabling Spoofing Resilience in GPS Receivers: One of the limitations of the GPS receiver design presented in Chapter 6 is it is only capable of detecting a spoofing attack. Even though detecting all known spoofing attacks is a significant improvement over the state of the art, the ability to annihilate or neutralize the attacker's spoofing signal will enable the receiver to continue operation even in the scenario of an attack. In the case of SPREE, the significant challenge in canceling the spoofing signal is the ability to determine the source of the auxiliary peak. For example, SPREE will raise an alarm once it detects an auxiliary peak. However, SPREE is incapable of identifying the exact peak that is caused by the attacker's spoofing signal. Given the ability to identify the spoofing signal's auxiliary peak, SPREE can retrieve its correct position and time from the legitimate GPS signals even in the scenarios of a spoofing attack. Building such a receiver needs to be further explored and investigated.

7.3 Final Remarks

In this thesis, we described the need for secure localization and demonstrated the fundamental limits of modern ranging and positioning systems. In order to build a secure localization system, one cannot rely on unidirectional or broadcast communication techniques such as GPS. We believe that a challenge-response mechanism such as distance bounding is a fundamental requirement for secure distance estimation. Although unidirectional or broadcast communication based ranging schemes such as GPS is convenient to use and allows systems to scale, they are inherently vulnerable to spoofing attacks. Furthermore, even if these systems are cryptographically protected, they are still vulnerable to message replay attacks. Countermeasures such as SPREE only make it harder for an attacker to succeed by imposing tighter constraints. However, there is a bound to securing such broadcast based localization systems and all countermeasures will either only provide limited protection or result in unreliable detection, for example, generate a large number of false positives. Thus, we conclude this thesis by asserting the need for designing technologies that enable secure localization and proximity verification for existing and future applications from the ground up.

Bibliography

[1] Apple Pay. https://www.apple.com/apple-pay/.

[2] Chaos Computer Club breaks Apple TouchID. http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.

[3] Ettus Research LLC. http://www.ettus.com/.

[4] GSG-xx Series Multi-channel advanced GNSS simulator. http://www.spectracomcorp.com/.

[5] Hacking A Phone's GPS May Have Just Got Easier. http://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/.

[6] LabSat GPS Simulator. http://www.labsat.co.uk/.

[7] Mini-Circuits. http://www.minicircuits.com.

[8] NASA's archive of space geodesy data. http://cddis.gsfc.nasa.gov/.

[9] NSL Primo GNSS SDR Front End. http://www.nsl.eu.com/primo.html.

[10] RF Ranging. http://www.rfranging.com/. Accessed: 2016-04-09.

[11] SPREE Source Code. http://www.spree-gnss.ch/.

[12] SX3 GNSS Software Receiver. http://www.ifen.com.

[13] UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea.

[14] Real Time Location Systems White Paper Version 1.02. Technical report, 2007.

[15] ISO/IEC 14443: Identification cards – Contactless integrated circuit cards – Proximity cards – Part 2: Radio frequency power and signal interface, 2010.

[16] 3db Access AG. Proximity based access control. `http://www.3db-technologies.com/`. Accessed: 2016-04-09.

[17] D. Adamy. *EW 101: a first course in electronic warfare*. Artech House, 2001.

[18] H.-S. Ahn, H. Hur, and W.-S. Choi. One-way ranging technique for CSS-based indoor localization. In *Proceedings of the 6th IEEE International Conference on Industrial Informatics*, 2008.

[19] D. M. Akos. Who's afraid of the spoofer? GPS/GNSS spoofing detection via automatic gain control (AGC). *Navigation*, 2012.

[20] Analog Devices. *AD8314 - RF Detector and Controller*.

[21] Atmel. Ultra Low Power 2.4GHz Transceiver for IEEE 802.15.4, ZigBee, and ISM Applications. `http://www.atmel.com/devices/AT86RF233.aspx`.

[22] P. Bahl and V. N. Padmanabhan. RADAR: an in-building RF-based user location and tracking system. In *Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies*, 2000.

[23] F. Bastide, D. Akos, C. Macabiau, and B. Roturier. Automatic gain control (AGC) as an interference assessment tool. In *ION GPS/GNSS 2003, 16th International Technical Meeting of the Satellite Division of The Institute of Navigation*, 2003.

[24] S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier, and J.-J. Quisquater. Secure implementation of identification systems. *Journal of Cryptology*, 1991.

[25] A. Bensky. *Wireless positioning technologies and applications.* Artech House, 2007.

[26] A. J. Berni and W. D. Gregg. On the Utility of Chirp Modulation for Digital Signaling. *IEEE Transactions on Communications*, 1973.

[27] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson. Chip and Skim: cloning EMV cards with the pre-play attack. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2014.

[28] K. Borre, D. M. Akos, N. Bertelsen, P. Rinder, and S. H. Jensen. *A software-defined GPS and Galileo receiver: a single-frequency approach.* Springer Science & Business Media, 2007.

[29] I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Secure and lightweight distance-bounding. In *Lightweight Cryptography for Security and Privacy*. Springer, 2013.

[30] I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Towards secure distance bounding. In *Fast Software Encryption*. Springer, 2013.

[31] I. Boureanu, A. Mitrokotsa, and S. Vaudenay. Practical and provably secure distance-bounding. *Journal of Computer Security*, 2015.

[32] M. S. Braasch. Performance comparison of multipath mitigating receiver architectures. In *Proceedings of the Aerospace Conference*. IEEE, 2001.

[33] S. Brands and D. Chaum. Distance-bounding protocols. In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, 1993.

[34] A. Broumandan, A. Jafarnia-Jahromi, V. Dehghanian, J. Nielsen, and G. Lachapelle. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In *Proceedings of the IEEE Position Location and Navigation Symposium (PLANS)*, 2012.

[35] N. Bulusu, J. Heidemann, and D. Estrin. GPS-less low-cost outdoor localization for very small devices. *Personal Communications*, 2000.

[36] L. Bussard and W. Bagga. Distance-Bounding Proof of Knowledge to Avoid Real-Time Attacks. In *Proceedings of 20th International Conference on Security and Privacy in the Age of Ubiquitous Computing*, 2005.

[37] S. Capkun, L. Buttyán, and J.-P. Hubaux. Sector: secure tracking of node encounters in multi-hop wireless networks. In *Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN)*, 2003.

[38] J. T. Chiang, J. J. Haas, J. Choi, and Y.-C. Hu. Secure location verification using simultaneous multilateration. *IEEE Transactions on Wireless Communications*, 2012.

[39] J. Clulow, G. Hancke, M. Kuhn, and T. Moore. So Near and Yet So Far: Distance-Bounding Attacks in Wireless Networks. In *Proceedings of the 3rd European Workshop on Security and Privacy in Ad-Hoc and Sensor Networks*. 2006.

[40] C. E. Cook and M. Bernfeld. *Radar signals: An introduction to theory and application*. Academic Press, New York, 1967.

[41] C. Cremers, K. B. Rasmussen, B. Schmidt, and S. Capkun. Distance Hijacking Attacks on Distance Bounding Protocols. In *Proceedings of the 33rd IEEE Symposium on Security and Privacy*, 2012.

[42] D. Dardari and R. D'Errico. Passive ultrawide bandwidth RFID. In *Proceedings of the IEEE Global Telecommunications Conference*, 2008.

[43] D. S. Dayton. FM "Chirp" Communications: Multiple Access to Dispersive Channels. *IEEE Transactions on Electromagnetic Compatibility*, 1968.

[44] DecaWave. DW1000 Product Description and Applications.

[45] F. Dehmas, G. Masson, and L. Ouvry. UWB Receiver with Time Drift Correction, 2015. US Patent 20,150,303,991.

[46] Y. Desmedt, C. Goutier, and S. Bengio. Special Uses and Abuses of the Fiat-Shamir Passport Protocol. In *CRYPTO*, 1987.

[47] D. Dolev and A. C. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 1983.

[48] EMVCo. Book A: Architecture and General Requirements, 2014. `http://www.emvco.com/specifications.aspx`.

[49] EMVCo. Book D: EMV Contactless Communication Protocol Specification, 2014. `http://www.emvco.com/specifications.aspx`.

[50] B. D. Farnsworth and D. W. Taylor. High precision narrow-band RF ranging. In *Proceedings of the International Technical Meeting of The Institute of Navigation*, 2010.

[51] J. Farrell and M. Barth. *The Global Positioning System and inertial navigation*. McGraw-Hill New York, 1999.

[52] C. Fernández–Prades, J. Arribas, P. Closas, C. Avilés, and L. Esteve. GNSS-SDR: An open source tool for researchers and developers. In *Proceedings of the ION GNSS Conference*, 2011.

[53] I. Fernández-Hernández, V. Rijmen, G. Seco-Granados, J. Simon, I. Rodríguez, and J. D. Calle. A Navigation Message Authentication Proposal for the Galileo Open Service. *Navigation*, 2016.

[54] C. Fischer and H. Gellersen. Location and Navigation Support for Emergency Responders: A Survey. *IEEE Pervasive Computing*, 2010.

[55] M. Fischlin and C. Onete. Terrorism in distance bounding: modeling terrorist-fraud resistance. In *Applied Cryptography and Network Security*. Springer, 2013.

[56] M. Flury, M. Poturalski, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec. Effectiveness of Distance-Decreasing Attacks Against Impulse Radio Ranging. In *Proceedings of the 3rd ACM Conference on Wireless Network Security*, 2010.

[57] A. Francillon, B. Danev, and S. Capkun. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. In *Proceedings of the 18th Annual Network and Distributed System Security Symposium*, 2011.

[58] L. Francis, G. Hancke, K. Mayes, and K. Markantonakis. On the security issues of NFC enabled mobile phones. *International Journal of Internet Technology and Secured Transactions*, 2010.

[59] S. Gambs, C. Onete, and J.-M. Robert. Prover anonymous and deniable distance-bounding authentication. In *Proceedings of the 9th ACM symposium on Information, computer and communications security*. ACM, 2014.

[60] L. Girod and D. Estrin. Robust range estimation using acoustic and multimodal sensing. In *Proceedings of the International Conference on Intelligent Robots and Systems*. IEEE, 2001.

[61] G. Gott and A. Karia. Differential Phase-Shift Keying Applied to Chirp Data Signals. *Proceedings of the Institution of Electrical Engineers*, 1974.

[62] S. K. S. Gupta, T. Mukherjee, K. Venkatasubramanian, and T. B. Taylor. Proximity Based Access Control in Smart-Emergency Departments. In *Proceedings of the 4th Annual IEEE International Conference on Pervasive Computing and Communications Workshops*, 2006.

[63] R. W. Hamming. Error Detecting And Error Correcting Codes. *Bell System Technical Journal*, 1950.

[64] G. P. Hancke. Practical attacks on proximity identification systems. In *Proceedings of the IEEE Symposium on Security and Privacy*, 2006.

[65] G. P. Hancke. Design of a secure distance-bounding channel for RFID. *Journal of Network and Computer Applications*, 2011.

[66] G. P. Hancke. Distance-bounding for rfid: Effectiveness of 'terrorist fraud' in the presence of bit errors. In *Proceedings of the IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*. IEEE, 2012.

[67] G. P. Hancke and M. G. Kuhn. An RFID distance bounding protocol. In *Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, 2005.

[68] G. P. Hancke and M. G. Kuhn. Attacks on time-of-flight Distance Bounding Channels. In *Proceedings of the 1st ACM Conference on Wireless Network Security*, 2008.

[69] S. Hengstler, D. P. Kasilingam, and A. H. Costa. A Novel Chirp Modulation Spread Spectrum Technique for Multiple Access. In *Proceedings of 7th IEEE International Symposium on Spread Spectrum Techniques and Applications*, 2002.

[70] J. Hermans, R. Peeters, and C. Onete. Efficient, secure, private distance bounding without key updates. In *Proceedings of the sixth ACM Conference on Security and privacy in wireless and mobile networks*. ACM, 2013.

[71] J. Hightower, R. Want, and G. Borriello. SpotON: An indoor 3D location sensing technology based on RF signal strength. *UW CSE*

00-02-02, University of Washington, Department of Computer Science and Engineering, Seattle, WA, 2000.

[72] W. Hirt. The European UWB radio regulatory and standards framework: Overview and implications. In *Proceedings of the IEEE International Conference on Ultra-Wideband*, 2007.

[73] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle. *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more*. Springer Science & Business Media, 2007.

[74] T. E. Humphreys. Detection strategy for cryptographic GNSS anti-spoofing. *IEEE Transactions on Aerospace and Electronic Systems*, 2013.

[75] T. E. Humphreys, J. A. Bhatti, D. P. Shepard, and K. D. Wesson. The Texas Spoofing Test Battery: Toward a standard for evaluating GNSS signal authentication techniques. In *Proceedings of the ION GNSS Meeting*, 2012.

[76] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner Jr. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Proceedings of the ION GNSS international technical meeting of the satellite division*, 2008.

[77] The Institute of Electrical and Electronic Engineers. *IEEE 802.15.4a-2007 Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs)*, 2007.

[78] The Institute of Electrical and Electronic Engineers. *ISO/IEC 24730-5 Information technology – Real-time locating systems (RTLS) – Part 5: Chirp spread spectrum (CSS) at 2.4 GHz air interface*, 2010.

[79] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle. GPS vulnerability to spoofing threats and a review of antispoofing techniques. *International Journal of Navigation and Observation*, 2012.

[80] A. J. Kerns, K. D. Wesson, and T. E. Humphreys. A blueprint for civil GPS navigation message authentication. In *Proceedings of the IEEE/ION Symposium on Position, Location and Navigation Symposium (PLANS)*, 2014.

[81] H. Kılınç and S. Vaudenay. Optimal proximity proofs revisited. In *Applied Cryptography and Network Security*. Springer, 2015.

[82] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira. The Swiss-Knife RFID Distance Bounding Protocol. In *Information Security and Cryptology — ICISC 2008*. 2008.

[83] J.-E. Kim, J. Kang, D. Kim, Y. Ko, and J. Kim. IEEE 802.15.4a CSS-based localization system for wireless sensor networks. In *Proceedings of the 4th IEEE International Conference on Mobile Adhoc and Sensor Systems*, 2007.

[84] S.-H. Kong. Statistical analysis of urban GPS multipaths and pseudo-range measurement errors. *IEEE Transactions on Aerospace and Electronic Systems*, 2011.

[85] M. G. Kuhn. An asymmetric security mechanism for navigation signals. In *Information Hiding*, 2005.

[86] B. M. Ledvina, W. J. Bencze, B. Galusha, and I. Miller. An in-line anti-spoofing device for legacy civil GPS receivers. In *Proceedings of the International Technical Meeting of the Institute of Navigation*, 2010.

[87] S. Lee, J. S. Kim, S. J. Hong, and J. Kim. Distance bounding with delayed responses. *Communications Letters, IEEE*, 2012.

[88] A. Lehner and A. Steingass. The land mobile satellite navigation multipath channel–a statistical analysis. In *Proceedings of the 2nd Workshop on Positioning, Navigation and Communication (WPNC) & 1st Ultra-Wideband Expert Talk (UET)*, 2005.

[89] G. Li, D. Arnitz, R. Ebelt, U. Muehlmann, K. Witrisal, and M. Vossiek. Bandwidth dependence of CW ranging to UHF RFID tags in severe multipath environments. In *Proceedings of the IEEE International Conference on RFID*, 2011.

[90] Linear Technology. *LTC5564 - UltraFast 7ns Response Time 15GHz RF Power Detector with Comparator*. `http://www.linear.com/docs/30075`.

[91] H. Liu, H. Darabi, P. Banerjee, and J. Liu. Survey of Wireless Indoor Positioning Techniques and Systems. *IEEE Transactions on Systems, Man, and Cybernetics*, 2007.

[92] S. C. Lo and P. K. Enge. Authenticating aviation augmentation system broadcasts. 2010.

[93] D. Manandhar, R. Shibasaki, and H. Torimoto. GPS reflected signal analysis using software receiver. *Journal on Positioning*, 2006.

[94] H. Matthews. *Surface wave filters: Design, construction, and use*. 1977.

[95] R. Miesen, F. Kirsch, P. Groeschel, and M. Vossiek. Phase based multi carrier ranging for UHF RFID. In *Proceedings of the IEEE International Conference on Wireless Information Technology and Systems (ICWITS)*, 2012.

[96] P. Misra and P. Enge. *Global Positioning System: Signals, Measurements, and Performance*. 2006.

[97] P. Misra and P. Enge. *Global Positioning System: Signals, Measurements and Performance Second Edition*. Lincoln, MA: Ganga-Jamuna Press, 2006.

[98] P. Y. Montgomery, T. E. Humphreys, and B. M. Ledvina. Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer. In *Proceedings of the ION International Technical Meeting*, 2009.

[99] J. Munilla and A. Peinado. Distance bounding protocols for RFID enhanced by using void-challenges and analysis in noisy channels. *ACM Journal on Wireless Communications and Mobile Computing*, 2008.

[100] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond. Chip and pin is broken. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, 2010.

[101] Y. J. Nam and Y.-G. Park. Efficient Indoor Localization and Navigation with a Combination of Ultrasonic and CSS-based IEEE 802.15.4a. In *Proceedings of the 4th International Conference on Ubiquitous Information Technologies Applications*, 2009.

[102] Nanotron Technologies GmbH. *NanoLOC TRX Transceiver (NA5TR1) User Guide Version 2.0*, 2008.

[103] Nanotron Technologies GmbH. *NanoLOC TRX Transceiver (NA5TR1) Datasheet Version 2.3*, 2010.

[104] T. Nighswander, B. M. Ledvina, J. Diamond, R. Brumley, and D. Brumley. GPS software attacks. In *Proceedings of the ACM Conference on Computer and Communications Security*, 2012.

[105] E. Pagnin, A. Yang, G. Hancke, and A. Mitrokotsa. HB+ DB, mitigating man-in-the-middle attacks against HB+ with distance bounding. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015.

[106] P. Papadimitratos and A. Jovanovic. GNSS-based Positioning: Attacks and countermeasures. In *Proceedings of the IEEE Military Communications Conference, MILCOM.*, 2008.

[107] J. Peck. SONAR–The RADAR of the Deep. In *Popular Science*. 1945.

[108] R. E. Phelts. *Multicorrelator techniques for robust mitigation of threats to GPS signal quality*. PhD thesis, Stanford University, 2001.

[109] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec. The Cicada Attack: Degradation and Denial of Service in IR Ranging. In *Proceedings of the IEEE International Conference on Ultra-Wideband*, 2010.

[110] M. Poturalski, M. Flury, P. Papadimitratos, J.-P. Hubaux, and J.-Y. L. Boudec. Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures. *IEEE Transactions on Wireless Communications*, 2011.

[111] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard, and T. E. Humphreys. Civilian GPS spoofing detection based on dual-receiver correlation of military signals. *Institute of Navigation GNSS (ION GNSS)*, 2011.

[112] M. L. Psiaki, S. P. Powell, and B. W. O'Hanlon. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In *Proceedings of the ION GNSS+ Meeting*, 2013.

[113] T. D. PulsON. 400 RCM. `http://www.timedomain.com/`. Accessed: 2016-04-09.

[114] C. S. J. Rabaey and K. Langendoen. Robust positioning algorithms for distributed ad-hoc wireless sensor networks. In *Proceedings of the USENIX Annual Technical Conference*, 2002.

[115] A. Ranganathan, N. O. Tippenhauer, B. Škorić, D. Singelée, and S. Capkun. Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System. In *Proceedings of the 17th European Conference on Research in Computer Security*. 2012.

[116] T. S. Rappaport. *Wireless communications: principles and practice*. 1996.

[117] K. B. Rasmussen and S. Capkun. Location Privacy of Distance Bounding Protocols. In *Proceedings of the 15th ACM conference on Computer and Communications Security*, 2008.

[118] K. B. Rasmussen and S. Capkun. Realization of RF Distance Bounding. In *Proceedings of the 19th USENIX Security Symposium*, 2010.

[119] 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*, 2009.

[120] 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*, 2007.

[121] M. Roland. Applying recent secure element relay attack scenarios to the real world: Google wallet relay attack. *Computing Research Repository*, 2012.

[122] Z. Sahinoglu and S. Gezici. Ranging in the IEEE 802.15.4a Standard. In *Proceedings of IEEE Annual Wireless and Microwave Technology Conference*, 2006.

[123] Z. Sahinoglu, S. Gezici, and I. Güvenc. *Ultra-wideband Positioning Systems: Theoretical Limits, Ranging Algorithms, and Protocols*. 2008.

[124] D. Salido-Monzú, E. Martin-Gorostiza, J. Lazaro-Galilea, F. Domingo-Perez, and A. Wieser. Multipath mitigation for a phase-based infrared ranging system applied to indoor positioning. In *Proceedings of the IEEE International Conference on Indoor Positioning and Indoor Navigation (IPIN)*, 2013.

[125] N. Sastry, U. Shankar, and D. Wagner. Secure verification of location claims. In *Proceedings of the 2nd ACM workshop on Wireless Security*, 2003.

[126] A. Savvides, H. Park, and M. B. Srivastava. The bits and flops of the n-hop multilateration primitive for node localization problems. In *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*. ACM, 2002.

[127] S. Sedighpour, S. Capkun, S. Ganeriwal, and M. B. Srivastava. Distance enlargement and reduction attacks on ultrasound ranging. In *Proceedings of the 3rd ACM Conference on Embedded Networked Sensor Systems*, 2005.

[128] D. Seetharam and R. Fletcher. Battery-Powered RFID. In *Proceedings of the 1st ACM Workshop on Convergence of RFID and Wireless Sensor Networks and their Applications*, 2007.

[129] D. Singelée, R. Peeters, and B. Preneel. Toward more secure and reliable access control. *IEEE Pervasive Computing*, 2012.

[130] D. Singelée and B. Preneel. Distance bounding in noisy environments. In *Proceedings of the 4th European Conference on Security and Privacy in Ad-hoc and Sensor Networks*, 2007.

[131] M. I. Skolnik. Introduction to RADAR. *Radar Handbook*, 1962.

[132] A. Springer, W. Gugler, M. Huemer, R. Koller, and R. Weigel. A Wireless Spread-Spectrum Communication System Using SAW Chirped Delay Lines. *IEEE Transactions on Microwave Theory and Techniques*, 2001.

[133] A. Springer, W. Gugler, M. Huemer, L. Reindl, C. C. W. Ruppel, and R. Weigel. Spread Spectrum Communications Using Chirp Signals. In *Proceedings of the IEEE/AFCEA Conference on Information Systems for Enhanced Public Safety and Security (EUROCOMM)*, 2000.

[134] A. G. Stove. Linear FMCW radar techniques. *Radar and Signal Processing, IEE Proceedings F*, 1992.

[135] A. Strobel and F. Ellinger. An active pulsed reflector circuit for fmcw radar application based on the switched injection-locked oscillator principle. In *Proceedings of the Semiconductor Conference Dresden (SCD)*, 2011.

[136] N. O. Tippenhauer. *Physical-Layer Security Aspects of Wireless Localization.* PhD thesis, ETH Zurich, Switzerland, 2012.

[137] N. O. Tippenhauer and S. Capkun. ID-based Secure Distance Bounding and Localization. In *Proceedings of the 14th European Conference on Research in Computer Security*, 2009.

[138] 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*, 2015.

[139] 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*, 2011.

[140] D. Titterton, J. Weston, et al. *Strapdown Inertial Navigation Technology. 2nd Edition.* IET, 2004.

[141] Y.-J. Tu and S. Piramuthu. RFID Distance Bounding Protocols. In *First International EURASIP Workshop on RFID Technology*, 2007.

[142] Ubisense Technologies. *Ubisense Real-time Location Systems (RTLS)*, 2010.

[143] S. Vaudenay. On modeling terrorist frauds. In *Provable Security*. Springer, 2013.

[144] S. Vaudenay. Private and secure public-key distance bounding. In *Financial Cryptography and Data Security*. Springer, 2015.

[145] M. Vossiek, R. Roskosch, and P. Heide. Precise 3-D Object Position Tracking using FMCW Radar. In *Proceedings of the 29th European Microwave Conference*, 1999.

[146] J. S. Warner and R. G. Johnston. GPS spoofing countermeasures. *Homeland Security Journal*, 2003.

[147] S. Wehrli, R. Gierlich, J. Hüttner, D. Barras, F. Ellinger, and H. Jäckel. Integrated Active Pulsed Reflector for an Indoor Local Positioning System. *IEEE Transactions on Microwave Theory and Techniques*, 2010.

[148] J. Wendel, O. Meister, C. Schlaile, and G. F. Trommer. An integrated GPS/MEMS-IMU navigation system for an autonomous helicopter. *Aerospace Science and Technology*, 2006.

[149] K. Wesson, M. Rothlisberger, and T. Humphreys. Practical cryptographic civil GPS signal authentication. *Journal of Navigation*, 2012.

[150] K. Wesson, D. Shepard, J. Bhatti, and T. E. Humphreys. An evaluation of the vestigial signal defense for civil GPS anti-spoofing. In *Proceedings of the ION GNSS Meeting*, 2011.

[151] K. D. Wesson. *Secure navigation and timing without local storage of secret keys*. PhD thesis, 2014.

[152] K. Whitehouse, C. Karlof, and D. Culler. A practical evaluation of radio signal strength for ranging-based localization. *ACM SIGMOBILE Mobile Computing and Communications Review*, 2007.

[153] M. Winkler. Chirp signals for communications. In *WESCON Convention Record*, 1962.

[154] Z. Xiang, S. Song, J. Chen, H. Wang, J. Huang, and X. Gao. A wireless LAN-based indoor positioning technology. *IBM Journal of Research and Development*, 2004.

[155] C. Yoon and H. Cha. Experimental analysis of IEEE 802.15.4a CSS ranging and its implications. *Computer Communications*, 2011.

[156] Zebra Technologies. *Sapphire Dart Ultra-Wideband (UWB) Real Time Locating System*, 2010.

[157] Y. Zhang, W. Qi, and S. Zhang. The unambiguous distance in a phase-based ranging system with hopping frequencies. *arXiv preprint arXiv:1403.1923*, 2014.