Proximity Verification for Contactless Access Control and Authentication Systems

ABSTRACT

Today, contactless smart cards are used to provide physical access control and authentication in a wide variety of applications. Prior research have demonstrated the vulnerability of contactless smart cards to relay attacks. For example, an attacker can relay the communication between the card reader and the smart card to steal a car or pay for goods in a supermarket. To solve this problem, smart cards need to be enhanced with secure proximity verification, i.e., distance bounding, which enables the card reader and the card to verify their mutual distance. However, existing technologies do not support the deployment of distance bounding in such systems: NFC cannot provide sufficient distance resolution, and hardware complexity of the proposed (e.g., UWB-based) distance bounding radios prevents their use in contactless smart cards.

In this work, 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 against 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.

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. Majority of these smart cards use radio frequency based 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 [1], NFC phones [2], Google Wallet [3]). 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 [4] i.e., with the ability to securely verify a device's proximity to the verifying terminal or reader. Distance bounding protocols enable the secure measurement of an upper bound on the physical distance between two devices, a verifier and a prover. In the case of access control systems, the reader and the card act as the verifier and the prover respectively. 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.

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 [5]. 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). Although a number of distance bounding protocols [6–12] were proposed after it was initially introduced in the context of wired systems [4], very few practical implementations exist. Some prior works on prover design focused on using analog or hybrid digital-analog processing in order to reduce the prover processing time to few nanoseconds [8, 13], but the hardware com-

plexity, storage requirements and power consumption at the side of the prover limit their use in contactless applications. Another line of work considered the implementation of distance bounding using ultra-wide band (UWB) signals with well defined physical-layer characteristics [14]. Although IR-UWB can estimate distances with centimeter level precision, processing IR-UWB pulses consumes significant amount of power (typically around $1 - 4$ W) making it unsuitable for use in applications such as contactless access control and authentication systems (or payment systems) where power consumption at the prover needs to be low (order of few mW or μW).

Additionally, with the advent of internet of things, a large number of interconnected sensors and actuators are expected to collect and exchange information. These *things* can be implanted heart monitors that sends continuous data to the patient's mobile phone, automobile sensors monitoring tyre 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 work, 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 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.

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 $124 - 135$ KHz low-frequency and 13.56 MHz high-frequency

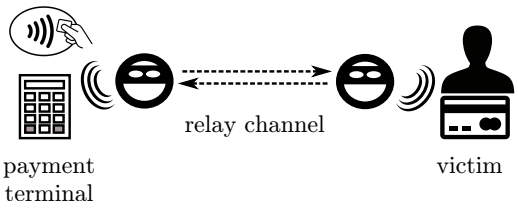

Figure 1: An attacker relays the communications between a legitimate contactless payment terminal and a card using two proxy devices.

(HF) bands are the most commonly used ones. Some systems also use the ultra-high frequency ($902 - 928$ MHz and $860-880$ MHz) and the microwave bands ($2400-2483.5$ MHz and $5725 - 5850$ 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 Internet of Things (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 [19, 20], relay attacks [21] do not require 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 1). Hancke [22] practically demonstrated the attack using specialized hardware as the proxy reader and card over a distance of 50 m. Later, Francis et al. [2] demonstrated that relay attacks can be executed using commodity phones equipped with NFC without the need of 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. [1] 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

Implementation	Attack Resilience			Compatible Protocols	Complexity[b]
	DF (processing delay)[a]	MF	TF		
Tippenhauer [14]	✓ (100 ns)	✓	✓	Any	High
Hancke [16]	✓ (40 ns)	✓	×	HKP [7]	High
CRCS [8][c]	✓ (1 ns)	✓	×	CRCS	High
Ranganathan [13][c]	✓ (3 ns)	✓	✓	HKP based [9, 17, 18]	High
Our Work	✓ ([d])	✓	✓	Any	Low

[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.
[c] Focused primarily on reducing the prover's processing delay and used frequency switching to communicate data.
[d] The use of slots enables us to decouple the distance estimation from the processing delay.

Table 1: Comparison of the existing distance bounding implementations in prior art.

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, [3] 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 in his mobile device. The recently announced Apple Pay [23] 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 the following section, we give a brief overview of distance bounding and its state-of-art designs. We briefly discuss the pros and cons of integrating these distance bounding implementations into contactless smart card systems.

3. DISTANCE BOUNDING

3.1 Background

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 phase. 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-response pairs in order to estimate its upper distance bound to the prover. The distance d between the verifier and the prover is calculated using the equation $d = \frac{c.(\tau - t_p)}{2}$, where c is the speed of light ($3 \cdot 10^8$ 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: *Mafia Fraud*, *Distance Fraud* and *Terrorist Fraud* attacks. *Mafia fraud attacks* are similar to relay attacks [21]. 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.

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. In *terrorist fraud attacks*, an untrusted prover collaborates with an external attacker to convince the verifier that he is closer than he really is. In this attack, the prover aids the external attacker without revealing his long term secret key. Recently, another type of attack on distance bounding protocols called the *distance hijacking* attack was proposed [25]. The attacker exploits an honest prover's presence by hijacking its rapid bit-exchange phase with the verifier. A system's resilience to distance hijacking depends on the higher level protocol implementation and is independent of the physical-layer.

3.2 Distance Bounding Implementations

A number of distance bounding protocols were proposed following the work of Brands and Chaum [4]. These protocols provide resilience against one or all of the above mentioned attacks. However, the security of these protocols was 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. For example, in time-of-flight based distance measurement systems, a 1 ns error in estimation results in a ranging error of 15 cm. Therefore, in practice, the security of distance bounding protocols also depends on the actual physical layer design and implementation of the distance bounding system.

Below we summarize the existing physical layer related designs available in the open literature. Initial distance bounding implementations [26, 27] proposed the use of both radio

[1] In some use cases, the authentication is based on TouchID, which has already been proven insecure [24].

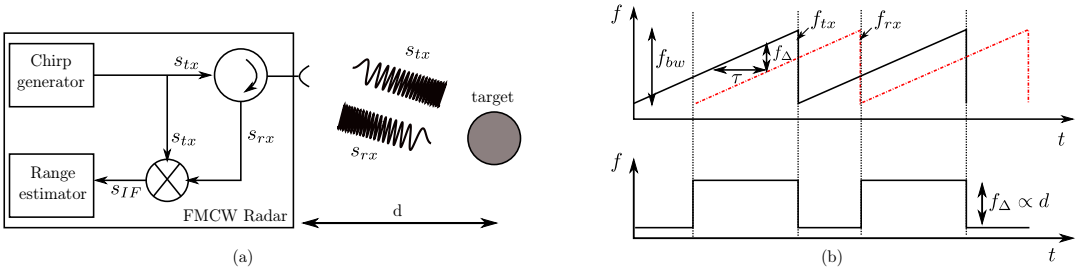

Figure 2: (a) Conventional FMCW-based radar system comprising of a chirp generator, mixer and a signal processing block to estimate range. (b) Ranging principle: The beat frequency f_Δ is the difference between the instantaneous transmit frequency and the frequency of the reflected signal. This beat frequency is proportional to the round-trip time delay τ for the signal to be received after being reflected off the target object.

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. 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 methods to reduce the prover's complexity and processing delay.

Ultrawide Band Distance Bounding Systems.

Hancke and Kuhn [7] introduced one of the first distance bounding protocols suitable for computationally constrained devices such as RFID with a specific prover design. Subsequently, Hancke [16] further extended this work with a UWB communication channel. In the proposed channel, the verifier (here the reader) embeds the challenge bits as ultra-wideband pulses in addition to the transmitted carrier signal. Since the communication link includes both the low-frequency carrier and the ultra-wideband pulses, the RFID tag receiver architecture complexity increases drastically. Tippenhauer [14] designed and implemented a distance bounding system with focus on optimizing the rapid bit-exchange phase. Due to the ranging precision and resilience to multipath effects, an impulse radio ultra-wideband (IR-UWB) physical layer was used for communication. IR-UWB 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. UWB-IR based ranging systems provide high distance measurement precision (of the order of few centimeters). However, the narrow IR-UWB pulses utilize a large bandwidth (>500 MHz) and therefore require high sampling rate ADCs and DACs to receive and transmit IR-UWB pulses respectively. Such high sampling rate ADCs and DACs consume significant power (typically around $1-4$ W) and increase system complexity.

Fast Prover Designs.

The main focus of these designs was to minimize the processing delay at the prover. The Challenge Reflection with Channel Selection (CRCS) [8] scheme reduced the prover's processing delay to 1 ns by eliminating the need for interpreting the challenge during the rapid-bit exchange phase. In this implementation, the challenges are reflected back by the prover on different frequency channels. 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, Hancke-Kuhn) cannot be realized using this scheme. In addition, the lack of challenge demodulation made this scheme vulnerable to terrorist fraud attacks. To solve this, Ranganathan et al. [13] proposed a hybrid analog-digital prover design that is resilient to terrorist fraud attacks with a prover processing delay of approximately 3 ns. This design can be used to implement all distance bounding protocols that follow the Hancke-Kuhn protocol construction i.e., the response is selected from one or more registers based on the challenge. Both works focused on minimizing the challenge processing delay at the prover through architectural modifications with very few details on the physical layer characteristics of the radio frequency signal which plays a critical role in ranging precision and data communication. 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. This increases the prover's memory requirements and thus its complexity, making it challenging to realize power-efficient, light-weight provers. We summarize and compare the aforementioned implementations in Table 1. Our work is motivated by the limitations of existing distance bounding radio designs i.e., limited compatibility with higher level protocols, inability to resist against strong attackers capable of early detection and late commit (more details in Section 5), complex verifier and prover designs and in certain cases high memory requirements. These limitations make them unsuitable for integration with many access control and authentication applications. In this work, we fill this void by proposing a distance bounding system, specifically designed for use in contactless access control and authentication systems.

4. FMCW BASED DISTANCE BOUNDING

4.1 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

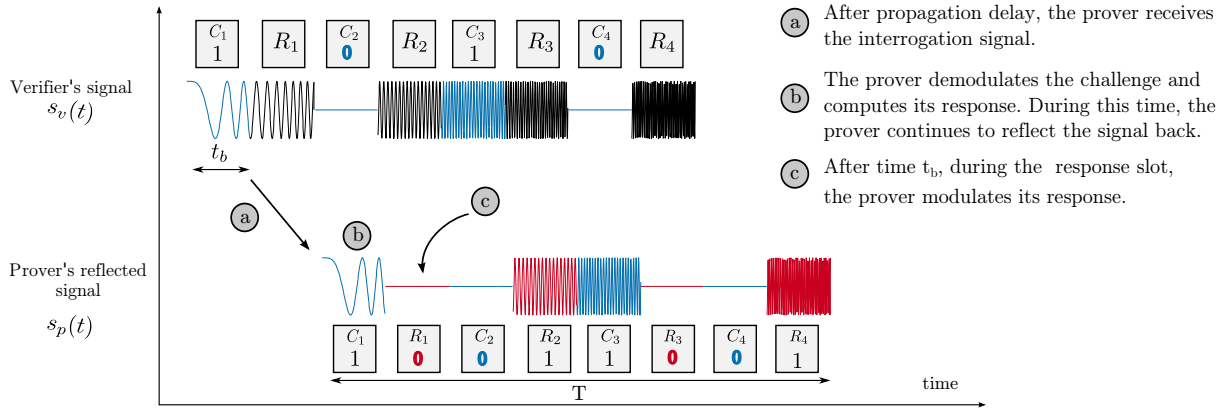

Figure 3: An example signal as transmitted by the verifier (reader) and the corresponding reflected signal from the prover (contactless card). The shown signals are for challenge bits $c[n] = \{1, 0, 1, 0\}$ and the prover's processing function is a simple "invert" operation. The verifier and prover synchronize to these slots using a preamble (not shown in figure).

radars are more susceptible to channel interference. In Frequency Modulated Continuous Wave (FMCW) radar [28], chirp signals [29] are used to determine range and velocity of a target. Figure 2(a) 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; thus enables measurement of distance d to the target object. The distance d is measured using the equation

$$d = \frac{c \cdot f_\Delta \cdot T}{2 \cdot f_{bw}} \tag{1}$$

where T is the duration of the chirp and f_{bw} is the bandwidth.

4.2 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

$$\sum_{n=1}^{N} c[n] \cdot \text{rect}(t - nt_b) s_{tx}(t) \tag{2}$$

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 (1). We describe the system design in more detail in the next sections.

4.3 Verifier and Prover Design

Figure 4 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.

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 3). 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 prior art 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 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 4 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

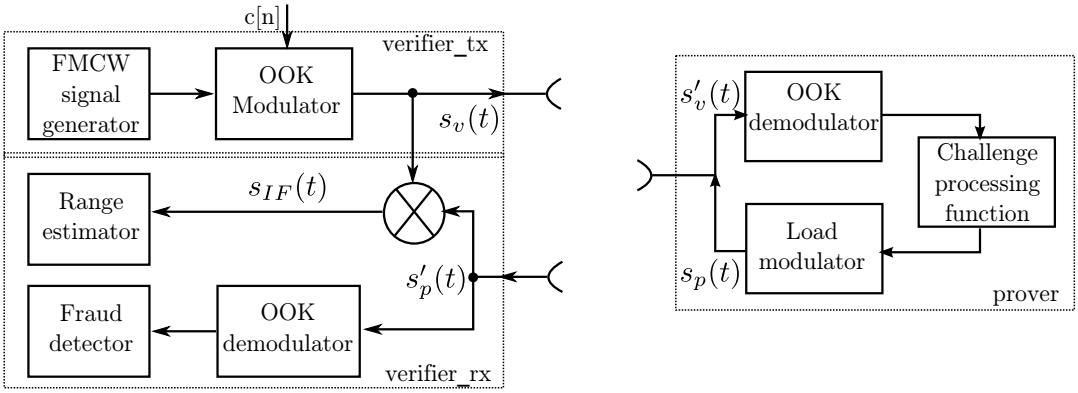

Figure 4: OOK-FMCW based distance bounding system architecture: The interrogating signal $s_v(t)$ is an OOK-FMCW transmitted by the verifier. The prover receives, demodulates the challenge and computes the response while simultaneously reflecting the challenge signal back to the verifier. The responses 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.

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.

5. SECURITY ANALYSIS

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

5.1 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 a 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. [5] 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 [30]. 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, lets 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,

$$t_{mafia} = 1.5t_b - 2t_{ed} - t_{hw} \tag{3}$$

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,

$$t_{mafia} = 0.5t_b - 2t_{ed} - t_{hw} \tag{4}$$

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

$$d_{gain} = \frac{c}{2} \cdot (0.5t_b - 2t_{ed} - t_{hw}) \tag{5}$$

It is important to note that Equation (5) 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

[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.

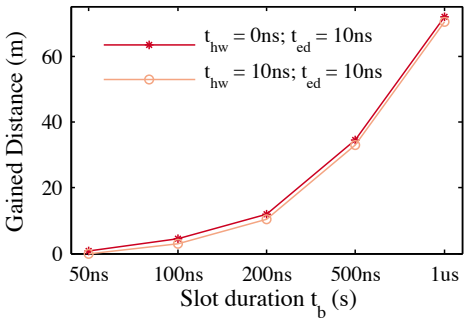

Figure 5: Maximum distance an attacker can cheat by performing an early-detect and late-commit attack on the physical layer of the symbol.

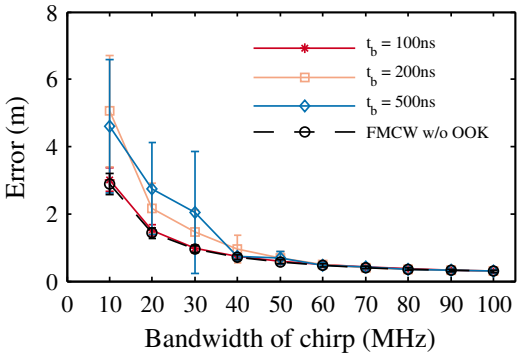

Figure 6: Measurement precision: The mean error in distance estimation against bandwidth of the FMCW signal for various slot durations t_b. The SNR was fixed at 15 dB and the error is a mean value obtained by measuring 100 different distances within the possible maximum measurable distance.

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.

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 6.3) 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, we give an intuition by substituting nominal values for t_{ed} and t_{hw}.

5.2 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 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 [9, 17, 18] 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.

6. 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.

6.1 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 μs 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 '0's and '1's 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 implemented following the theory described in Section 4.1.

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 $t_b = 100$ 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 6. 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.

6.2 Experimental Setup

Our experiments primarily focuses 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 7. 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 generated using Matlab as described in Section 6.1 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 [31] 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.

6.3 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 8(a) 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.

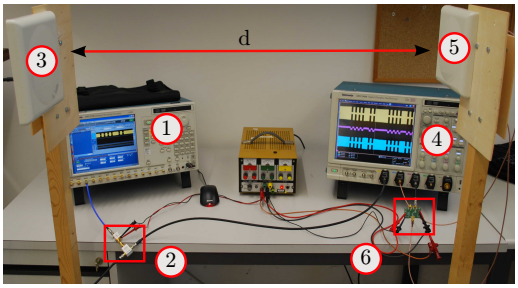

Figure 7: An arbitrary waveform generator (1) outputs the OOK-FMCW samples. The signal is amplified (2) and a part of it is transmitted using a planar antenna (3) and the other recorded for distance estimation using a storage oscilloscope (4). The received signal (5) is input to the OOK detection and inverter circuit (6) and to the storage oscilloscope.

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 4.1 and the results are plotted in Figure 8(b). 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 [32]. The results illustrate that for an allowed ISM bandwidth of 80 MHz, the ranging uncertainty in a severe multipath environment was around 1 m and improved with higher sweep bandwidth.

7. 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 [31,33] 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 6.2) responds within 25 ns and can

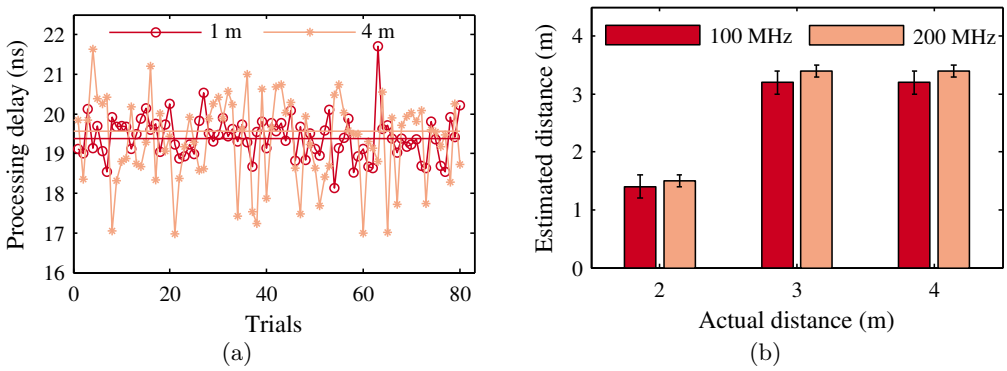

Figure 8: (a) Challenge processing delays. The median value of t_p was approximately 19.5 ns for both the values of $d = \{1\,\text{m}, 4\,\text{m}\}$. (b) Ranging precision. For $d = \{2, 3, 4\}$ m, the errors in the estimated distances were less than a meter.

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., [34–37]) 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 [38] is also possible.

Alternate design choices: The resilience of the proposed FMCW-based distance bounding system to ED and LC attacks can be improved in the following ways: (i) Frequency analysis of the backscatter signal at the verifier and (ii) phase modulation of responses at the prover. 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. A late commit attack would result in incorrect bin values appearing consistently throughout the chirp sweep bandwidth and hence can be used in detection. 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 allow 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.

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

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

9. REFERENCES

[1] A. Francillon, B. Danev, and S. Ĉapkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," in *Proceedings of the 18th Annual Network and Distributed System Security Symposium*. The Internet Society, Feb. 2011.

[2] 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*, vol. 2, Dec. 2010.

[3] M. Roland, "Applying recent secure element relay attack scenarios to the real world: Google wallet relay attack," *Computing Research Repository*, vol. abs/1209.0875, 2012.

[4] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, ser. EUROCRYPT '93. Springer-Verlag New York, Inc., May 1993, pp. 344–359.

[5] 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*, ser. Lecture Notes in Computer Science. Springer, Sep. 2006, pp. 83–97.

[6] N. O. Tippenhauer and S. Čapkun, "ID-based Secure Distance Bounding and Localization," in *Proceedings of the 14th European Conference on Research in Computer Security*. Berlin, Heidelberg: Springer-Verlag, Sep. 2009, pp. 621–636.

[7] 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*, Sep. 2005, pp. 67–73.

[8] K. B. Rasmussen and S. Čapkun, "Realization of RF Distance Bounding," in *Proceedings of the 19th USENIX Security Symposium*, Aug. 2010, pp. 389–402.

[9] 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*, Mar. 2007, pp. 204–213.

[10] 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*, May 2005, pp. 223–238.

[11] S. Capkun, L. Buttyán, and J.-P. Hubaux, "Sector: secure tracking of node encounters in multi-hop wireless networks," in *Workshop on Security of Ad Hoc and Sensor Networks (SASN)*. ACM, Oct. 2003, pp. 21–32.

[12] 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*. Berlin, Heidelberg: Springer-Verlag, Jul. 2007, pp. 101–115.

[13] A. Ranganathan, N. O. Tippenhauer, B. Škorić, D. Singelée, and S. Capkun, "Design and Implementation of a Terrorist Fraud Resilient Distance Bounding System," in *Computer Security – ESORICS 2012*, ser. Lecture Notes in Computer Science. Springer, Sep. 2012, vol. 7459, pp. 415–432.

[14] N. O. Tippenhauer, "Physical-Layer Security Aspects of Wireless Localization," Ph.D. dissertation, ETH Zurich, Switzerland, 2012.

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

[16] G. P. Hancke, "Design of a secure distance-bounding channel for RFID," *J. Netw. Comput. Appl.*, vol. 34, no. 3, pp. 877–887, May 2011.

[17] 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*. Berlin, Heidelberg: Springer-Verlag, Dec. 2009, pp. 98–115.

[18] Y.-J. Tu and S. Piramuthu, "RFID Distance Bounding Protocols," in *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, Sep. 2007.

[19] M. Bond, O. Choudary, S. J. Murdoch, S. Skorobogatov, and R. Anderson, "Chip and Skim: cloning EMV cards with the pre-play attack," 2014.

[20] S. J. Murdoch, S. Drimer, R. Anderson, and M. Bond, "Chip and pin is broken," in *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 433–446.

[21] Y. Desmedt, C. Goutier, and S. Bengio, "Special Uses and Abuses of the Fiat-Shamir Passport Protocol," in *CRYPTO*, Aug. 1987, pp. 21–39.

[22] G. P. Hancke, "Practical attacks on proximity identification systems," in *Security and Privacy, 2006 IEEE Symposium on*. IEEE, 2006, pp. 6–pp.

[23] "Apple pay," https://www.apple.com/apple-pay/.

[24] "Chaos computer club breaks apple touchid," http://www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.

[25] 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*, May 2012.

[26] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proceedings of the 2nd ACM workshop on Wireless Security*. New York, NY, USA: ACM, Sep. 2003, pp. 1–10.

[27] K. B. Rasmussen and S. Čapkun, "Location Privacy of Distance Bounding Protocols," in *Proceedings of the 15th ACM conference on Computer and Communications Security*, Oct. 2008, pp. 149–160.

[28] A. G. Stove, "Linear FMCW radar techniques," *Radar and Signal Processing, IEE Proceedings F*, vol. 139, no. 5, pp. 343–350, Oct. 1992.

[29] A. J. Berni and W. D. Gregg, "On the Utility of Chirp Modulation for Digital Signaling," *IEEE Transactions on Communications*, vol. 21, no. 6, pp. 748–751, Jun. 1973.

[30] 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*. ACM, Apr. 2008, pp. 194–202.

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

[32] 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 *RFID (RFID), 2011 IEEE International Conference on*. IEEE, 2011, pp. 19–25.

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

[34] D. Dardari and R. D'Errico, "Passive ultrawide bandwidth rfid," in *Global Telecommunications Conference, 2008. IEEE GLOBECOM 2008. IEEE*. IEEE, 2008, pp. 1–6.

[35] D. Seetharam and R. Fletcher, "Battery-powered rfid," in *1st ACM Workshop on Convergence of RFID and Wireless Sensor Networks and their Applications*, 2007.

[36] 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*, vol. 58, no. 2, pp. 267–276, Feb. 2010.

[37] A. Strobel and F. Ellinger, "An active pulsed reflector circuit for fmcw radar application based on the switched injection-locked oscillator principle," in *Semiconductor Conference Dresden (SCD), 2011*, Sep. 2011, pp. 1–4.

[38] W. Hirt, "The european uwb radio regulatory and standards framework: Overview and implications," in *Ultra-Wideband, 2007. ICUWB 2007. IEEE International Conference on*. IEEE, 2007, pp. 733–738.