Physical-Layer Attacks on Chirp-based Ranging Systems

Aanjhan Ranganathan*
aanjhan.ranganathan@inf.ethz.ch

Boris Danev*
boris.danev@inf.ethz.ch

Aurélien Francillon†
aurelien.francillon@eurecom.fr

Srdjan Capkun*
srdjan.capkun@inf.ethz.ch

* ETH Zurich
Department of Computer Science
8092 Zurich, Switzerland

† Eurecom
2229 Route des Cretes
F-06560 Sophia-Antipolis

ABSTRACT

Chirp signals have been extensively used in radar and sonar systems to determine distance, velocity and angular position of objects and in wireless communications as a spread spectrum technique to provide robustness and high processing gain. Recently, several standards have adopted chirp spread spectrum (CSS) as an underlying physical-layer scheme for precise, low-power and low-complexity real-time localization. While CSS-based ranging and localization solutions have been implemented and deployed, their security has so far not been analyzed.

In this work, we analyze CSS-based ranging and localization systems. We focus on distance decreasing relay attacks that have proven detrimental for the security of proximity-based access control systems (e.g., passive vehicle keyless entry and start systems). We describe a set of distance decreasing attacks realizations and verify their feasibility by simulations and experiments on a commercial ranging system. Our results demonstrate that an attacker is able to effectively reduce the distance measured by chirp-based ranging systems from 150 m to 700 m depending on chirp configuration. Finally, we discuss possible countermeasures against these attacks.

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection

Keywords

Chirp, Ranging Systems, Physical-layer attacks

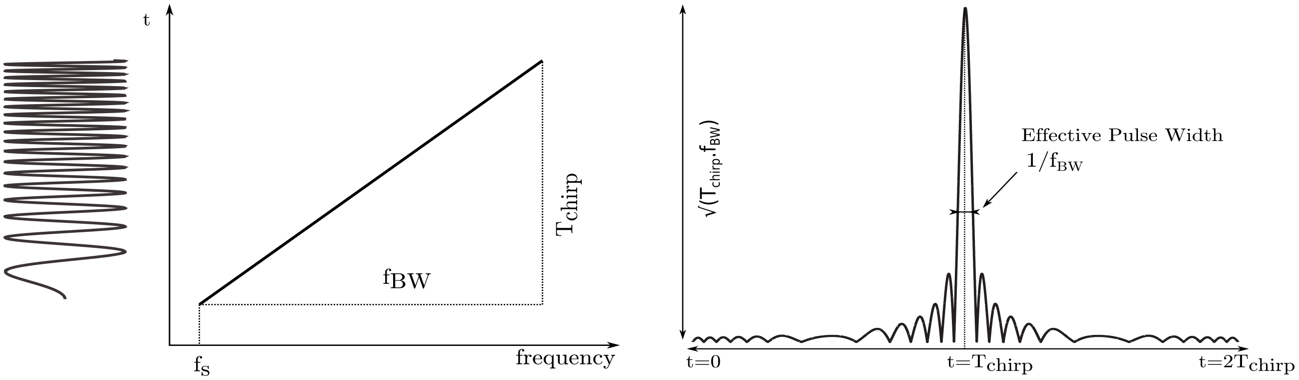
1. INTRODUCTION

The rapid deployment of wireless systems has driven an increasing interest in the use of radio communication technologies for ranging and localization. The combination of data communication and location determination enables a broad application space of location-aware services [19]. Examples include people localization and tracking, asset management as well as safety and security applications such as emergency support [11] and access control [16, 33].

Numerous ranging and localization technologies were developed in the last decade [24]; 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 [26] for outdoor localization and systems based on RSS [6, 44], TDOA [41, 46] and round-trip time-of-flight (RTOF) [42, 3] 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 [37]. For short and medium-distance precision ranging and localisation, ultra-wide band (UWB) and chirp spread spectrum (CSS) emerged as the most prominent techniques and were standardized in IEEE 802.15.4a [21] and ISO/IEC 24730-5 [22]. Their ranging resolution and reliability makes them suitable for numerous applications including indoor asset tracking and guidance [36], loss protection [3], 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 [7, 39] allow low-complexity and low-power implementations of both the transmitter and receiver on a single integrated hardware [28]. This enables the realization of two-way distance-ranging solutions using RTOF with relatively high distance resolution (1 m) [3].

In this work, we study 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 appropriateness of use in security- and safety-critical applications has 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 [14], passive vehicle keyless entry

WiSec'12, April 16–18, 2012, Tucson, Arizona, USA.
Copyright 2012 ACM 978-1-4503-1265-3/12/04 ...$10.00.



(a) Frequency vs Time representation of chirp signal.

(b) Result of pulse compression.

Figure 1: Chirp signals: (a) The linear variation of chirp signal frequency with time. (b) Compressed pulse output of the matched filter.

systems [13]) further motivate the need of 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 [29]. 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 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 600 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 paper is organized as follows. In Section 2, we provide CSS background. In Section 3, we define and discuss the attacks that can be mounted on chirp-based ranging systems. In Section 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 5, we enumerate possible countermeasures. We provide the related work in Section 7 and conclude the paper in Section 8.

2. BACKGROUND: CHIRP SPREAD SPECTRUM

In this section we provide an overview of chirp signals and pulse compression commonly used by radar systems for distance measurement. We then describe typical chirp-based ranging and discuss the existing CSS standards and commercially available chirp-based ranging solutions.

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 [7] have been extensively used in radar and sonar systems [9, 30] 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 1 where f_s is the starting sweep frequency and θ_0 represents the initial phase of the signal. Figure 1(a) shows how the chirp signal changes in frequency with time. Equation 2 gives the sweep rate α of the signal in terms of the chirp duration T_{chirp} and chirp bandwidth ω_{BW}.

$$y(t) = sin[2\pi(f_s + \alpha \cdot t)t] \tag{1}$$

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

$$f(t) = f_s + \alpha \cdot t \tag{3}$$

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 matched filter output with a chirp input is a short pulse as shown in Figure 1(b). The pulse width of the chirp T_{chirp} is compressed to an effective width of $1/\omega_{BW}$. 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 multi-path and other channel disturbances. Another advantage is that chirps can be processed only using analog signal processing blocks e.g., SAW filters [38]. This allows low-complexity and low-power realization of both communication and ranging. The strong auto-correlation properties

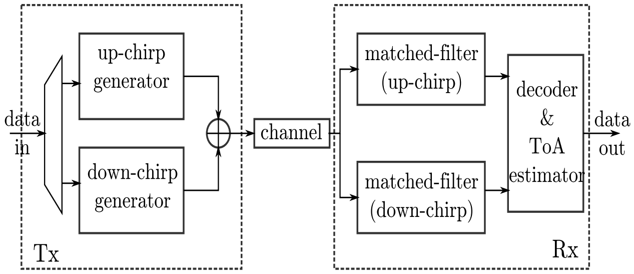


Figure 2: Building blocks of a CSS system: Data is modulated using BOK scheme at the transmitter. The receiver decodes and estimates time-of-arrival based on the matched filter outputs.

of the chirp signals add more robustness to distance measurements in multipath environments.

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.

2.2.1 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 [43], '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 [15, 20], 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 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.

2.2.2 TOA estimation and ranging

Distance 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.

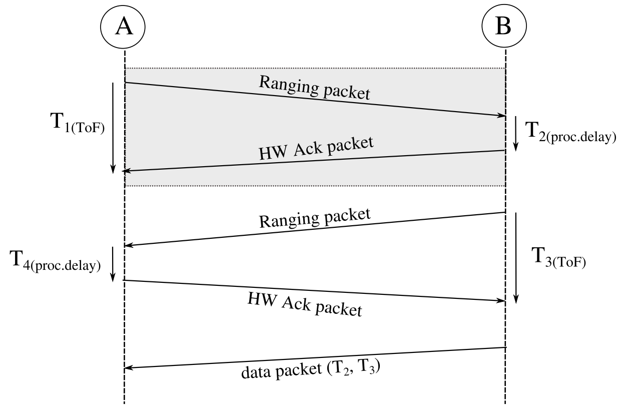


Figure 3: SDS-TWR ranging scheme: RTOF measurements $(T_{1(ToF)}, T_{3(ToF)})$ are calculated by both nodes A and B. In the final step node B exchanges its time measurements with A. In a single sided two way ranging (highlighted), the RTOF measurement is calculated by node A only.

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 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.

2.3 CSS Ranging Standards

In 2007, the IEEE 802.15.4a-2007 [21] standard was introduced to standardize lower network layers of wireless personal area networks with 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 [22] 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 4.0μs. The distance range is estimated based on the RTOF measurements. Local clock drifts introduces inaccuracies in the measurements. The 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 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.

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.

3.1 Distance Decreasing Attack by Early Detection and Late Commit

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* (ii) by an external attacker who aims 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 3. Moreover, device B can reduce its message processing time. The presented techniques in the reminder of this paper 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 [40, 34].

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. [8] introduced attacks using ED and LC and their feasibility on RFID was demonstrated in [18]. 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.

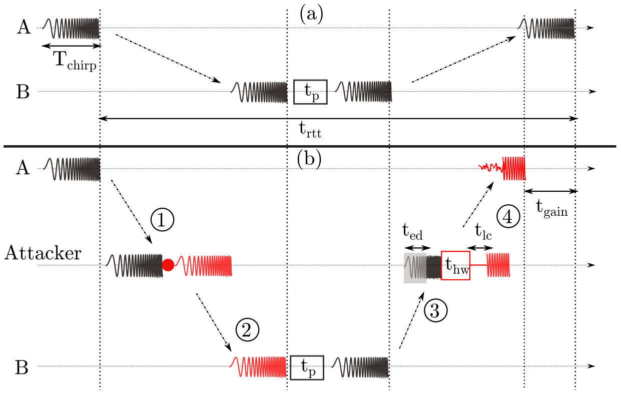
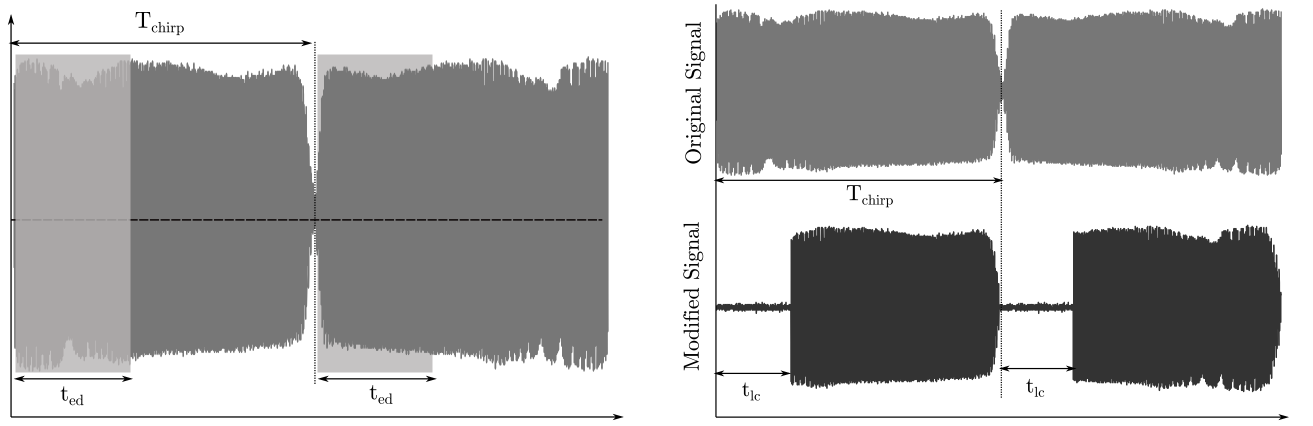


Figure 4: Distance decreasing attack: (a) CSS ranging in a non-adversial setting where t_{rtt} is the estimated RTOF. (b) Attacker reduces the total round-trip time to $t_{rtt} - t_{gain}$ by performing early detect and late commit on node B's response CSS signal while communications from A to B are relayed without any LC or ED.

Figure 4 illustrates how an attacker modifies the distance by means of early detect and late commit of CSS signals. Figure 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(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 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 to 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 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 5(a) and 5(b) respectively.

The attacker hardware circuitry for performing the early



(a) Signal properties of early detect.

(b) Signal properties of a late committed signal.

Figure 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.

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 $d_{gain} = c \cdot t_{gain}$. 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 the sum of all the above factors as follows.

$$t_{gain} = t_{lc} - t_{ed} - t_{hw} \tag{4}$$

In the following subsections, we discuss how to perform the aforementioned early detection and late commit attacks on CSS based ranging systems. In Section 4.3, we validate these attacks experimentally.

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 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 4.3.1.

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 digitising 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.

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 maximise 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 5(b) 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 4.3.2

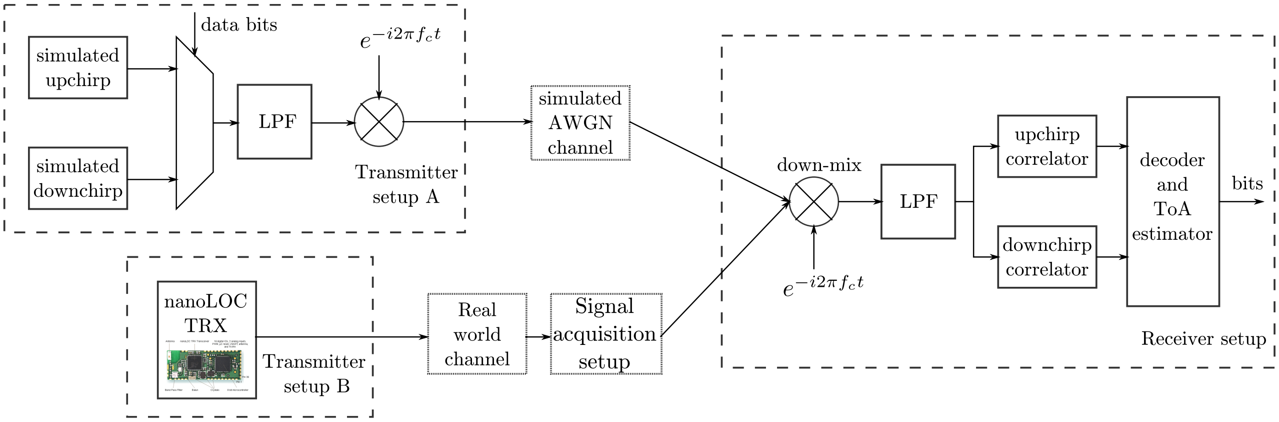


Figure 6: Experimental setup consisting of the simulated chirp transmitter (Transmitter setup A), the NanoLOC transceivers (Transmitter setup B) and the CSS receiver.

that the receiver is still able to decode the modified signal with an acceptable bit error rate.

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.

4.1 Experimental Setup

Our simulation and experimental setup (Figure 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 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 $T_{chirp} = \{1,\ 2,\ 4\}\ \mu$s. 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 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 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.

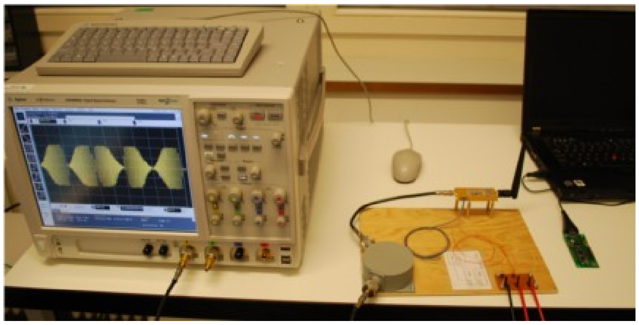


Figure 7: The signal acquisition setup for recording NanoLOC transciever CSS transmissions.

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 dB low-noise amplifier. The received signal is then digitized at RF by an oscilloscope where the data is sampled at 10 GSa/s and stored. Figure 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 m as shown in Figure 8.

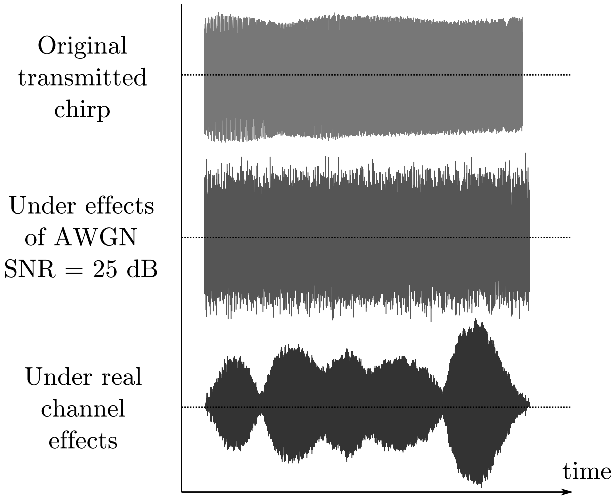


Figure 8: Comparison of the received CSS signal under an AWGN channel and real-world channels with that of the originally transmitted chirp.

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

Table 1: System parameters used in the analysis.

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.

4.3 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 gain.

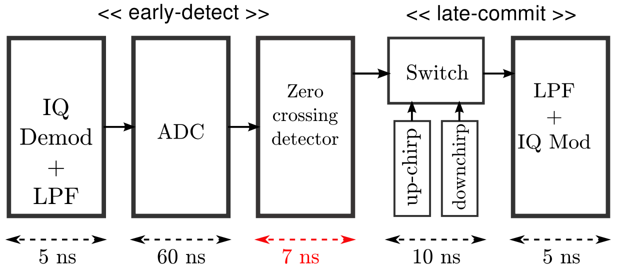


Figure 9: Attacker hardware: The zero crossing detector algorithm tested on a FPGA introduced a delay of 7 ns. Specified time delays of other blocks are based on COTS hardware specifications.

4.3.1 *Early detection of chirps*

We evaluate the feasibility of early detection using the zero crossing detector and short correlations (Section 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 in 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 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 10(a) 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 10(b). 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 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 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 10(c). 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.

4.3.2 Late commit attack

We evaluated the behaviour 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 11(a) and Figure 11(b) 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 behaviour 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 11(c).

4.3.3 Hardware implementation

The attacker's hardware delay influences the effective distance decrease. Figure 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 ($t_{hw} = 87\,\text{ns}$). We account for t_{hw} in our effective distance decrease estimates described in Section 4.3.5.

4.3.4 Effect of error correction coding schemes

Errors in wireless communications, e.g., due to channel fading are common. Error correcting codes add reduncdant 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 [17] 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 11(c) 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 distance decreasing attack. To this extent, from Figure 10(b) it would be sufficient to observe the chirp only for 10% of the chirp.

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

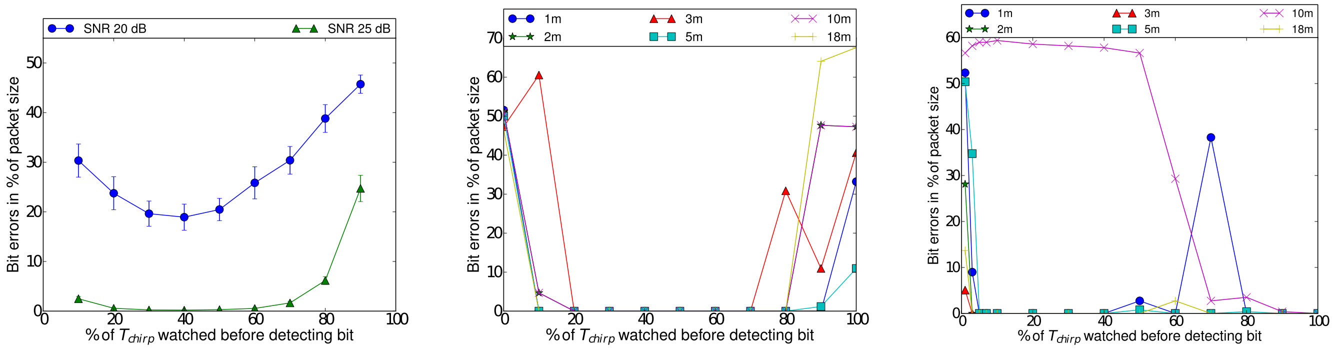
Table 2: Effective distance estimates.

4.3.5 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 3.1, the effective distance gained depends on three factors: (i) t_{ed} (ii) t_{lc} and (iii) t_{hw}. From Figure 10(b), the attacker is required to observe at least 20% of the chirp period to predict the symbol with 100% accuracy. Similarly, from Figure 11(c), an attacker can wait no longer than 80% of T_{chirp} for committing to a symbol. The attacker's hardware delay in Section 4.3.3 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 summarised in Table 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 600 m for 4μs long chirps. However, the use of error correcting codes increases the above estimates by about 10%.

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 are sweep all frequencies in a linear manner, a late commit 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 an 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 a effective way.

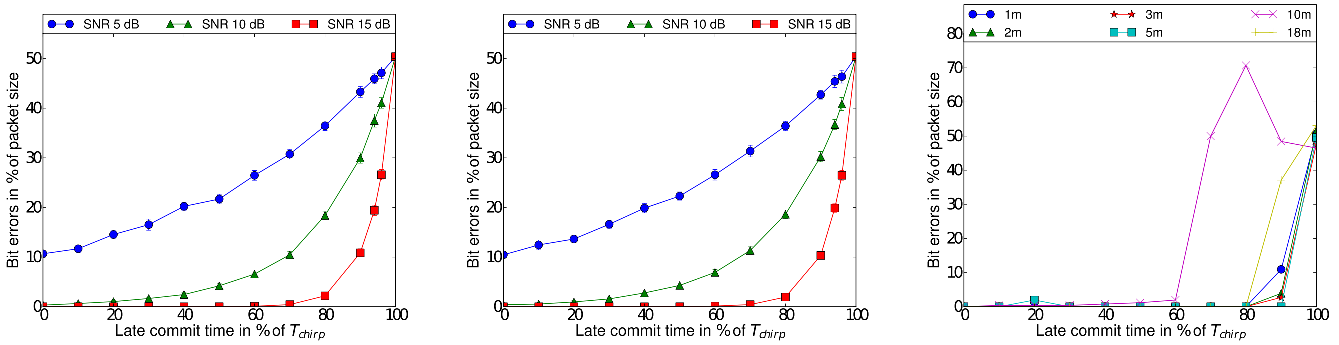


(a) Early detection of chirps on simulated AWGN channel.

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

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

Figure 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.



(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 11: Late commit receiver behaviour: (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}.

6. FUTURE WORK

In this work we analyzed CSS ranging systems that modulate data using BOK. The applicability of the ED and LC attacks on ranging systems implementing chirp direct modulation (CDM) needs further investigation. CDM systems primarily use chirps for spreading and modulate data using a m-ary PSK scheme. PSK-based systems encode data in the phase transitions between symbol periods. The time window available to early detect and late commit is therefore smaller than in a BOK scheme and thereby the possibility of distance decreasing attacks would depend on the particular synchronisation and decoding procedures. We intend to consider such techniques in future work.

Physical-layer attacks on ranging systems are highly time-constrained. Existing radio platforms such as USRP have a processing delay of the order of few microseconds (larger than symbol period) before the received signal is decoded; which makes them unsuitable without modification for implementing ED and LC attacks. We intend to realize an end-to-end hardware module with small processing delay and capable of executing physical-layer attacks in real-time as future work. Such a platform [2] would also enable real-world security analysis of proposed solutions.

7. 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 are 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 physical-layer security of wireless ranging systems beginning with the works closest to ours.

Clulow et al.[8] 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 [18]. Flury et al. [12, 32] 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. [31] introduced the Cicada attack on the impulse radio ultra wide-band PHY. In this attack, a malicious transmitter continuously transmits a "1" impulse with 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. [13] 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 an USRP [1].

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, 10]. David Adamy in [4] 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 [25]. 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 [27, 23, 5, 35]. Yoon et al. [45], 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.

8. CONCLUSIONS

In this paper we described 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 m for 1μ s chirps and approximately 600 m for 4μ s chirps. Future work needs to investigate the effectiveness of possible countermeasures as well as physical-layer attacks on other CSS-based schemes.

9. ACKNOWLEDGEMENTS

This work was funded by the Swiss National Science Foundation (SNSF) under the grant 200020_129605 and NCCR-MICS. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of SNSF or NCCR-MICS.

10. REFERENCES

[1] Ettus research llc. http://www.ettus.com/.

[2] QuiXilica TRITON VXS-V5 Digitizer. TEK Microsystems, Inc; *www.tekmicro.com.*

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

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

[5] H.-S. Ahn, H. Hur, and W.-S. Choi. One-way ranging technique for CSS-based indoor localization, July 2008.

[6] 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*, volume 2, pages 775–784, Mar. 2000.

[7] A. J. Berni and W. D. Gregg. On the Utility of Chirp Modulation for Digital Signaling. *IEEE Transactions on Communications*, 21(6):748–751, June 1973.

[8] 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*, Lecture Notes in Computer Science, pages 83–97. Springer, Sept. 2006.

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

[10] D. S. Dayton. FM "Chirp" Communications: Multiple Access to Dispersive Channels. *IEEE Transactions on Electromagnetic Compatibility*, (2):296–297, June 1968.

[11] C. Fischer and H. Gellersen. Location and Navigation Support for Emergency Responders: A Survey. *IEEE Pervasive Computing*, 9:38–47, Jan. 2010.

[12] 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*, pages 117–128. ACM, Mar. 2010.

[13] 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.

[14] 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*, 2, Dec. 2010.

[15] G. Gott and A. Karia. Differential Phase-Shift Keying Applied to Chirp Data Signals. *Proceedings of the Institution of Electrical Engineers*, 121(9):923–928, Sept. 1974.

[16] 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*, pages 512–516, Mar. 2006.

[17] R. W. Hamming. Error Detecting And Error Correcting Codes. *Bell System Technical Journal*, 29(2):147–160, 1950.

[18] 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, pages 194–202. ACM, Apr. 2008.

[19] M. Hazas, J. Scott, and J. Krumm. Location-aware computing comes of age. *IEEE Computer*, 37(2):95–97, Feb. 2004.

[20] S. Hengstler, D. P. Kasilingam, and A. H. Costa. A Novel Chirp Modulation Spread Spectrum Technique for Multiple Access. In *Proceedings of IEEE Seventh International Symposium on Spread Spectrum Techniques and Applications*, volume 1, pages 73–77, Sept. 2002.

[21] 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.

[22] 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.

[23] 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*, pages 1–3, Oct. 2007.

[24] H. Liu, H. Darabi, P. Banerjee, and J. Liu. Survey of Wireless Indoor Positioning Techniques and Systems. *IEEE Transactions on Systems, Man, and Cybernetics*, 37(6):1067–1080, Nov. 2007.

[25] H. Matthews. *Surface wave filters: Design, construction, and use*. New York, Wiley-Interscience, 1977.

[26] P. Misra and P. Enge. *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, 2006.

[27] 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*, pages 1–6, Dec. 2009.

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

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

[30] J. Peck. SONAR–The RADAR of the Deep. In *Popular Science*, volume 147. Nov. 1945.

[31] 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 2010 IEEE International Conference on Ultra-Wideband*, volume 2, pages 1–4, Sept. 2010.

[32] 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*, 10(4):1334–1344, Apr. 2011.

[33] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Čapkun. Proximity-based Access Control for Implantable Medical Devices. In *Proceedings of the 16th ACM conference on Computer and Communications Security*, pages 410–419. ACM, Nov. 2009.

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

[35] Z. Sahinoglu and S. Gezici. Ranging in the IEEE 802.15.4a Standard. In *Proceedings of 2006 IEEE Annual Wireless and Microwave Technology Conference*, pages 1–5, Dec. 2006.

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

[37] 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*, New York, NY, USA, Nov. 2005. ACM.

[38] 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*, 49(4):754–760, Apr. 2001.

[39] A. Springer, W. Gugler, M. Huemer, L. Reindl, C. C. W. Ruppel, and R. Weigel. Spread Spectrum Communications Using Chirp Signals. In *EUROCOMM 2000. Information Systems for Enhanced Public Safety and Security. IEEE/AFCEA*, pages 166–170, May 2000.

[40] 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*, pages 621–636, Berlin, Heidelberg, Sept. 2009. Springer-Verlag.

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

[42] M. Vossiek, R. Roskosch, and P. Heide. Precise 3-D Object Position Tracking using FMCW Radar. In *Proceedings of the 29th European Microwave Conference*, volume 1, pages 234–237, Oct. 1999.

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

[44] 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*, 48(5.6):617–626, Sept. 2004.

[45] C. Yoon and H. Cha. Experimental analysis of IEEE 802.15.4a CSS ranging and its implications. *Computer Communications*, 34(11):1361–1374, Feb. 2011.

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