Security of Multicarrier Time-of-Flight Ranging

Patrick Leu, Martin Kotuliak, Marc Roeschlin, Srdjan Čapkun
Department of Computer Science
ETH Zurich, Switzerland

ABSTRACT

OFDM is a widely used modulation scheme. It transmits data over multiple subcarriers in parallel, which provides high resilience against frequency-dependent channel drops (fading) and achieves high throughput. Due to the proliferation of OFDM-enabled devices and the increasing need for location information, the research community has suggested using OFDM symbols for secure (time-of-flight) distance measurements. However, a consequence of relying on multiple subcarriers is long symbols (time-wise). This makes OFDM systems not a natural fit for secure ranging, as long symbols allow an attacker longer observation and reaction times to mount a so-called early-detect/late-commit attack. Despite these concerns, a recent standardization effort (IEEE 802.11az [5]) envisions the use of OFDM-based signals for secure ranging. This paper lays the groundwork for analyzing OFDM time-of-flight measurements and studies the security guarantees of OFDM-based ranging against a physical-layer attacker. We use BPSK and 4-QAM, the most robust configurations, as examples to present a strategy that increases the chances for early-detecting the transmitted symbols. Our theoretical analysis and simulations show that such OFDM systems are vulnerable to early-detection/late-commit attacks, irrespective of frame length and number of subcarriers. We identify the underlying causes and explore a possible countermeasure, consisting of orthogonal noise and randomized phase.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

IEEE 802.11az, Secure Ranging, OFDM

ACM Reference Format:
Patrick Leu, Martin Kotuliak, Marc Roeschlin, Srdjan Čapkun. 2021. Security of Multicarrier Time-of-Flight Ranging. In *Annual Computer Security Applications Conference (ACSAC '21), December 6–10, 2021, Virtual Event, USA.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3485832.3485898

1 INTRODUCTION

Secure ranging is important for applications that rely on proximity (car lock) or positioning (navigation, autonomous driving). Recent proposals for secure distance measurements rely on ultra-wideband wireless communications (UWB) [3]. Even though transmitting on a wide frequency range can provide sub-10cm ranging precision and high security-guarantees, this technology is not yet widely deployed. Due to its use of wide segments of licensed spectrum, it is subject to stringent constraints on transmit power. Moreover, the fact that the signal power is compressed in short pulses makes amplification difficult and limits the distance for practical operation.

Compared to UWB, orthogonal frequency division multiplexing (OFDM) is a modulation technique that is widely used today, especially in wireless systems that offer high throughput, such as in WiFi or cellular (i.e., 4G, 5G). A lot of infrastructure supporting these communication standards has been deployed with an ongoing trend towards high-bandwidth OFDM signals (5G). With OFDM, data is transmitted over many subcarriers in parallel. This provides robustness against frequency-selective channel drops (fading) [18]. However, because the subcarriers are closely spaced in frequency in most OFDM-based systems, an OFDM receiver requires multiple time samples for correct decoding. The transmitted symbols are significantly longer than for most singlecarrier systems, which is not ideal for (secure) ranging. Over the last decade, there was a lot of research dedicated to overcoming this challenge and re-purposing OFDM signals in WiFi for time-of-flight (ToF)-based ranging and positioning [11, 14, 27], achieving ranging precision on the order of meters or less.

Such performance numbers are sufficient for many applications, and OFDM signals are a viable candidate for ranging. However, in the context of distance bounding and ranging, the security of OFDM systems is unclear to date, unlike ultra-wideband (UWB) based systems that are thought to be secure against a powerful, Dolev-Yao-like attacker with idealized reaction times [23]. Given the vast proliferation of OFDM systems today and in the foreseeable future (5G), it is therefore of great importance to also assess the security of OFDM-based ranging implementations. This concern has been identified by the ongoing IEEE 802.11az standardization effort for next-generation positioning based on WiFi signals. Current proposals for secure ranging that have been made by the respective Task Group [5] include different OFDM modulations where random symbol sequences are transmitted to acquire the time-of-flight (ToF).

At the time of writing this paper (June 2021), the Task Group has not yet decided on the final technique that would provide the most resilience against a distance-reducing attacker. The fact that discussions have been ongoing for more than four years [6] clearly indicates the challenging nature of OFDM-based ranging. Undoubtedly, one needs to fully understand the security implications of a ranging scheme before its design is "baked" into billions of hardware chips supporting the upcoming IEEE 802.11az standard.

In light of this development, we aim to identify the pitfalls of OFDM-based ranging and assess whether multicarrier time-of-flight ranging can be secure. We choose a theoretical angle to approach the question and assume an idealized adversary with no hardware

ACSAC '21, December 6–10, 2021, Virtual Event, USA

ACM ISBN 978-1-4503-8579-4/21/12…$15.00
https://doi.org/10.1145/3485832.3485898

constraints. Therefore, our results serve as a guideline for real-world systems that might relax the adversarial model by constraining reaction time, sensitivity, and computational power of a potential attacker. In addition to the theoretical insights, we make our own proposal for secure multicarrier ranging that is based on orthogonal noise and can be used in conjunction with other approaches..

In order to increase positioning accuracy, some OFDM-based ranging systems exploit signal phase and directionality alongside time-of-flight information. Since these features do not contribute to the system's overall security—phase information can easily be subverted, see, e.g., [21]—, the focus of this work will only be on the security guarantees provided by time-of-flight measurements.

In particular, we make the following contributions:

- We provide mathematical proof that robust OFDM constellations, namely BPSK and 4-QAM, are vulnerable to early-detection. An attacker can identify (almost) any symbol with access to only a quarter (plus one) of the time-domain samples for BPSK and half (plus one) of the time-domain samples for 4-QAM.
- For the highly performant BPSK, we constructively prove the existence of valid late-commit attack sequences for all non-pulsed symbols. Those factors jointly lead to a deterministically achievable, significant distance reduction.
- We identify a possible countermeasure that involves a continuous extension of the constellation grid.

The paper is organized as follows. The following Section 2 introduces secure ranging and summarizes the main results. Section 3 introduces the vulnerabilities of highly robust OFDM configurations. In Section 4, we address a potential countermeasure. We discuss our findings in a broader sense in Section 5 and provide related work in Section 6 before concluding in Section 7.

2 BACKGROUND AND SUMMARY OF RESULTS

Over the last two decades, OFDM and its variants have become the predominant modulation techniques for high-throughput wireless communication, both in the WiFi and cellular domains (4G, 5G). In the cellular domain, we see a trend towards high signal bandwidths (100MHz and more), which furthers the adoption of OFDM modulation and increases the utility of those signals for ranging based on time-of-flight measurement. The security of such systems against physical-layer attackers depends on certain time-domain properties of the modulation. However, due to the information being encoded in the frequency domain, the resulting physical-security properties against a distance-modifying attacker do not follow trivially and have, to the best of our knowledge, not been studied so far.

2.1 OFDM

Orthogonal frequency-division multiplexing encodes message bits in frequency domain and transforms them into time-domain by an inverse Fourier transform, i.e.,

$$\mathbf{c} = \mathcal{F}^{-1}\left\{\mathbf{C}\right\},$$

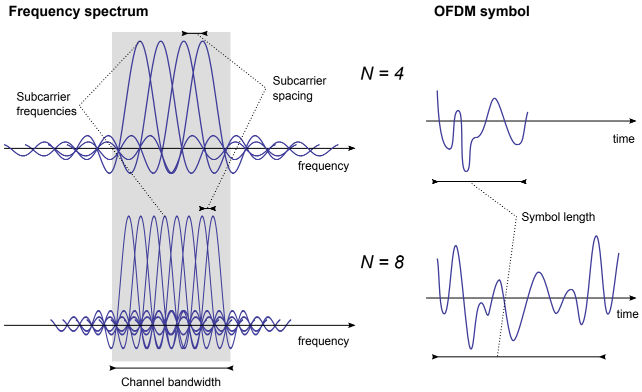

Figure 1: OFDM signal in frequency and time domain for different numbers of subcarriers (N). The frequency spectrum shows how the subcarriers share the channel bandwidth. The transmitter modulates message bits on individual subcarriers and applies an Inverse Fourier Transform to arrive at the time samples (on the right).

which is defined as

$$c_n = \sum_{k=0}^{n_s-1} C_k e^{\frac{i2\pi k}{n_s}n}.$$

The values of $\mathbf{C}$ are determined by the symbol bit-sequence $\mathbf{b}$ and the constellation mapping $MAP(\cdot)$, e.g., BPSK, QPSK, 16-QAM, etc. This results in the transmitted signal

$$\mathbf{c} = OFDM(\mathbf{b}) = \mathcal{F}^{-1}\left\{MAP(\mathbf{b})\right\},$$

which is sent over the wireless channel. The receiver then retrieves the information bits after performing an FFT on the incoming signal,

$$\mathbf{b}' = OFDM^{-1}(\mathbf{c}) = DEMAP\left(\mathcal{F}\left\{\mathbf{c}\right\}\right),$$

where the demapping operation is a hypothesis test based on the constellation set. As information bits are transmitted on orthogonal subcarriers (illustrated in Fig. 1), OFDM provides resilience to frequency-selective fading. The dips in the channel transfer function caused by fading remain constrained to a subset of the subcarriers. The receiver can maintain the orthogonality under a channel by adding a cyclic prefix (CP), which means to prepend the last few samples of the symbol at the beginning, thus circularizing the symbol. This allows simple equalization on a per-subcarrier level, as orthogonalization ensures an independent impact of the channel on each subcarrier.

To enable reliable communication, an OFDM transceiver has to perform additional tasks, namely synchronization, frequency and sampling offset correction, channel estimation and equalization. Introducing a cyclic prefix can help with those tasks. However, use of a cyclic prefix has a detrimental effect on ranging security. The cyclic prefix adds redundancy such that an attacker can predict the last part of the symbol with absolute certainty, even after only listening to the first part of the symbol (i.e., the cyclic prefix). For the remainder of this paper, we are therefore only concerned with "plain" OFDM symbols that neither contain a cyclic prefix, nor any guard symbols or bands. This is a realistic assumption, which has

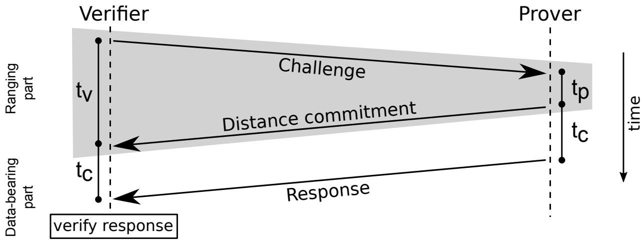

Figure 2: Time-of-flight (ToF) ranging with a known static distance commitment. ToF $= (t_v - t_p)/2$ **where** $t_p \ll t_c$ **are fixed parameters to accommodate hardware delay (**t_p**) and time to compute the response (**t_c**).**

Figure 3: Mafia Fraud attack scenario against distance bounding and ranging. The attacker tries to reduce the time-of-flight measurement acquired by the verifier.

also been made by the IEEE 802.11az standardization effort. When in ranging mode, OFDM symbols must not feature (additional) redundancy, such as a cyclic prefix.

2.2 Distance bounding and secure ranging

Typically, a distance-bounding or secure ranging protocol allows a prover to convince a verifier to be within a certain distance. Among the different techniques to measure physical distance based on a radio signal, time-of-flight measurement is the only one with the potential of being secure against a physical-layer attacker. This is based on the observation that an unknown signal's arrival time cannot be meaningfully modified (i.e., reduced) by an attacker, as opposed to the signal's absolute strength or phase. We focus on a scenario where two entities, a verifier and a prover, determine their distance by measuring the time-of-flight (ToF) of a signal exchange, as illustrated in Figure 2. We assume the prover to be trusted and, in particular, entrusted with maintaining a time schedule that feeds into ToF estimation. We will henceforth assume the use of a *distance commitment*, as presented in [25]. This allows us to separate the fast reply from the data-bearing part in a challenge-response protocol for secure ranging, removing the need for fast processing of the challenge, i.e., to decouple the time-critical part of the protocol, unlike rapid bit exchange in Brands and Chaum [8]. Alternatively, the reply time could even be communicated by the prover after the ranging exchange. Irrespective of this protocol design choice, the crucial requirement on the data-bearing part is that an attacker cannot advance the response in time through reactive interference.

2.2.1 Attacks against distance bounding and ranging. The research community has coined four attack scenarios in the context of distance-bounding protocols: Distance Fraud, Mafia Fraud, Terrorist Fraud, and Distance Hijacking [4]. In this work, we focus on Mafia Fraud, where both verifier and prover are honest, and an external attacker (a separate entity) attempts to modify the ToF measurement such that the prover appears to be closer to the verifier. Figure 3 visualizes the Mafia Fraud attack. This is also the attack scenario the IEEE 802.11az task group is mainly concerned with.

In order to achieve distance reduction, the attacker has to make sure the challenge message is registered at the prover at an earlier time than the legitimate challenge, and/or, advance both distance commitment and response message in a way that they arrive at the verifier at an earlier time. The attacker can operate either on the protocol/data-layer or on the symbol level to inject and advance the messages. If the adversary cannot predict the content of the messages, it is forced to resort to the symbol level and has to mount a so-called *early-detection/late-commit (ED/LC) attack*. We explain the ED/LC attack assuming the attacker attempts to advance the challenge message. The same technique can be applied to the response message.

For every symbol the verifier transmits, the attacker also emits a symbol, such that it arrives at the prover with a certain time advantage. Because the attacker does not know the exact symbol apriori, the first part of the adversarial symbol can be random noise, tricking the prover into believing that the wireless channel has distorted the start of the symbol. Figure 4 shows an abstract example of an ED/LC attack performed against a singlecarrier symbol. The adversary starts transmitting early even though the exact symbol is not known yet.

Since wireless transmission is not instant and the symbols have a certain duration, the attacker listens to the verifier's transmission (while interfering with the prover) and tries to detect the verifier's actual symbol based on the fraction of the signal received so far. This process is called early-detection (shown as ED in Fig. 4). Assuming the attacker succeeds and early-detects the verifier's symbol with high probability, it changes its own transmission from noise to a valid symbol—or a signal that is interpreted by the prover as the intended symbol[1]. This step of the attack is called late-commit (shown as LC in Fig. 4) and, if successful, makes the second part of the adversarial symbol appear as a valid symbol to the prover which blames the noise in the first part of the symbol on the channel and continues with the protocol. Finally, the attacker succeeds in reducing the time-of-flight measurement and in accomplishing the Mafia Fraud.

2.3 IEEE 802.11az

Within the IEEE 802.11az task group, there is an ongoing standardization effort towards secure OFDM-based ranging [5]. Publicly available, preliminary documents indicate that a physical-layer attacker is indeed considered a threat and part of the ongoing discussion. These documents discuss an attacker with limited reaction times and countermeasures evolving around coarser measures, such as avoiding cyclic prefixes and highly redundant encoding. Some of the documents treat a similar attacker as introduced in this work, operating on the sub-symbol level, however, without a rigorous study underpinning the presented measures. Our work aims to help

[1] The adversary superimposes its signal onto the legitimate signal. The adversarial signal has to take such effects into account and has to be transmitted at higher power for it to be decoded correctly at the receiver.

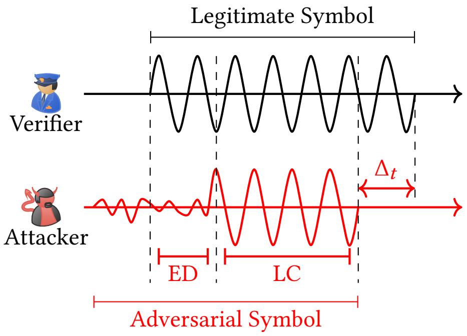

Figure 4: Concept of ED/LC attack: An attacker can reduce the measured time-of-arrival by identifying the symbol based on its initial samples and sending the later part of the symbol early.

bridge this gap and thus assist the standardization effort by providing a rigorous physical-layer analysis that can motivate the choice of the modulation for the symbol sequences used for ToA estimation. This allows extending the security argument to a physical-layer attacker that is not constrained with regard to reaction time.

2.4 Known principles clash with implementation and performance constraints

Low peak-to-average power ratio (PAPR) is an important signal property for performant operation in real-world systems. The reason is that fast changes in the signal (the opposite of low PAPR) are challenging to amplify without encountering non-linearities of the hardware, causing inter-carrier interference and limiting overall performance (i.e., communication distance). Due to power constraints, many end devices have amplifiers optimized for efficiency, which makes them, in turn, highly nonlinear. Therefore, OFDM uses different techniques to limit the PAPR. One of them is to limit the codeset and exclude high-PAPR symbols, of which pulses are the most extreme examples.

On the other hand, existing proposals for modulations enabling secure time-of-arrival measurement all assume pulses that are spaced by more than the channel delay-spread [16]. The existing understanding of secure physical layer design for ranging and the requirements on practical OFDM systems cannot be reconciled without either a heavy performance (data rate, range) penalty or hardware changes. E.g., [24] makes a proposal to use a multicarrier system like a single-carrier (UWB-like) system, a technique that provides security, however heavily constrains the information content per symbol and relies on time-domain techniques at the receiver. The question addressed in this work is to investigate the security of multicarrier modulations in general and whether we can find a technique that allows for secure ranging within the practical OFDM assumptions, those being parallel transmission on all subcarriers and frequency-domain mapping and demapping.

2.5 Summary of results

We show that the OFDM configurations that offer the highest robustness, i.e., BPSK and 4-QAM, are prone to ED/LC attacks. We provide mathematical proof that irrespective of the number of subcarriers, the first quarter and first half of the symbol allow the attacker to learn the full BPSK or 4-QAM symbol, respectively. In the case of BPSK, every symbol can be late-committed with only half the samples. For BPSK, the most robust constellation, the susceptibility to both early-detection and late-commit attack leads to a deterministically achievable distance reduction of more than 200m for a typical 802.11 OFDM configuration of 20MHz split into 64 subcarriers. In the case of 4-QAM, we show that an attacker's late-commit success can be significantly improved with an optimization technique, resulting in a considerable adversarial advantage in a distance-reducing attack. We identify the structure of the frequency-domain constellation grid as the main enabler of strong early-detection strategies and identify a technique that uses orthogonal noise and a random phase shift as a possible countermeasure since those operations limit structural information about the frequency-domain constellation.

3 THE OFDM ED/LC ATTACK

In the context of ToF distance measurement, it is well-known that an attacker can exploit the time-redundancy of symbols to decrease the measured distance, irrespective of cryptographic primitives [10, 19]. For example, if a modulation uses repetitions of a certain signal shape for improved robustness, an attacker can early-detect this symbol by only decoding the first repetition and can late-commit to such a symbol by only transmitting the last repetition. This behavior is illustrated in Figure 5. For the outcome of such an attack, it is not important whether the symbols are sent in direct succession or in separate frames. It is, however, not straightforward how such an attacker performs in OFDM since the symbols are encoded in the frequency domain and only before transmission transformed into a time-domain symbol. The physical-layer attacker presents us with a heavy asymmetry in the information-theoretic sense between the attacker's observation and the verifiable information at the receiver (prover and verifier). An attacker can "understand" and interact with the signal at the physical layer, while the receiver will only be able to assess the validity of the signal after demodulating it into bits. This demodulation must be robust against noise and multi-path channel propagation for reliable operations over long communication ranges, and we do not want to break with this requirement.

3.1 Attacker model

As mentioned in Section 2.2.1, we assume a Mafia Fraud attack scenario, where the external attacker is located between the two legitimate entities that measure their relative distance via signal time-of-flight (ToF). The attacker's goal is to decrease the measured time of arrival of the communication protocol employing an early-detect/late-commit (ED/LC) attack or a similar technique. While an attacker could also work on the protocol/data-layer, in the following, we constrain ourselves with an attacker that operates on the symbol level. If not taken care of at the physical layer, such an attacker can be successful irrespective of cryptographic primitives

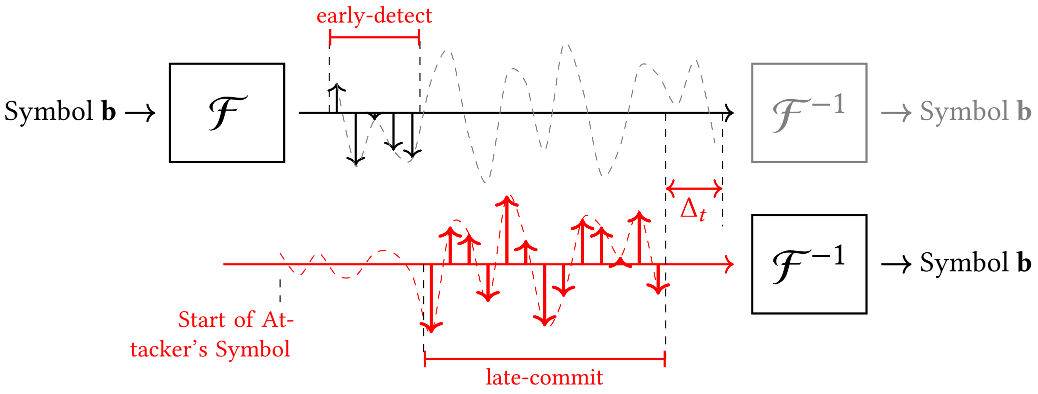

Figure 5: OFDM distance-reduction attack. If the attacker can understand the symbol based on a number of initial samples, he can send the late symbol preemptively and thereby achieve advancement (Δ_t) of the symbol (ED/LC attack). In the context of ToF ranging, this enables a distance-reduction attack.

and protocols (such as distance bounding) on higher layers. Moreover, we assume an attacker that can receive and react to signals at the physical layer at arbitrarily high sensitivity and arbitrarily small reaction times. We understand that this is an unattainable attacker model in the real world; however, in order to account for future technological advances, we do not want to limit ourselves to the current state-of-the-art results. As the attacker's aim is distance reduction, we assume the attacker has full control over his signal power, and the legitimate signal is negligible in relative power. This naturally applies in a scenario where the legitimate devices are out of communication range, however, an attacker can relay signals, e.g., by wire (relay attack). This provides the attacker the advantage of amplifying the signal as needed and, in particular, establishing a communication path, whereas in reality, the victim devices might be out of range. This attacker model is in line with the ones chosen in recent proposals for secure ToF estimation [16, 23].

3.2 Robust OFDM configurations

Performance-enhancing techniques such as channel compensation, cyclic prefix, and coding can create additional vulnerability to an ED/LC attacker since those techniques create dependencies between parts of the symbol. The absence of such techniques can be compensated by using highly robust constellations for the symbol sequences used for ToF estimation. For this reason, we cover the two most robust constellations in our analysis.

3.2.1 BPSK. Binary phase-shift keying (BPSK) uses a maximally robust symbol constellation. In BPSK, each subcarrier can only assume one of two possible values: +1 or -1. Robustness is an important characteristic and a key design goal on the bit sequences used for ranging in recent standardization efforts [3, 5]. Unfortunately, as opposed to the pulsed scenario, OFDM BPSK proves a particularly bad choice regarding a distance-reducing attacker, especially an early-detect late-commit (ED/LC) attacker. The reason is that a limited set of constellation points in frequency-domain results in strong time-domain *symmetry*. Because all n_s frequency-domain values are real, any BPSK symbol exhibits Hermitian symmetry in time-domain. This means the last $n_s/2 - 1$ time-domain samples are complex-conjugated versions of the $n_s/2 - 1$ samples after the initial sample c_0. Indeed, we will prove constructively that strong late-commit sequences exist for all non-pulse BPSK symbols, requiring an attacker to send only half the samples. In addition, we will see that the time-domain samples contain a substantial amount of differential information about the entire symbol, granting a steep learning curve to the early-detecting attacker.

3.2.2 4-QAM. 4-QAM is the minimal constellation that transmits bits on both signal-space dimensions in parallel, resulting in four possible constellation points per tone. As a consequence, it provides double the data rate, however at slightly less robustness under equal overall signal strength, compared to BPSK.

3.3 Early-detection

An early-detecting attacker is looking for the algorithm that will detect the correct message with highest probability, for a given detection delay δ_{ed}. The advantage of an early-detect algorithm *ED* at detection delay δ_{ed} over a symbol set $\mathcal{B}$ is defined as

$$A_{ED}(\mathcal{B}, \delta_{ed}) = \underset{\mathbf{b} \leftarrow \mathcal{B}}{P} \left(ED \left(\mathbf{c}_{ED} || 0^{(n_s - \delta_{ed})} \right) = \mathbf{b} \right),$$

where

$$\mathbf{c}_{ED} = c_0 || \ldots || c_{\delta_{ed}-1},$$

and

$$\mathbf{c} = OFDM\left(\mathbf{b}\right).$$

In the following, we introduce two different viewpoints on early-detection. The first is standard OFDM demodulation, which simply applies an FFT on the zero-padded time-domain signal before testing on the polarity of each tone. Then, we analyze a time-domain sample-by-sample matching strategy, assuming an attacker with optimal sensitivity. This second viewpoint shall grant insights into optimized strategies, e.g., strategies that compensate for inter-carrier-interference (ICI) imposed by the fact that later time-domain samples are unknown, an effect that highly impacts standard demodulation.

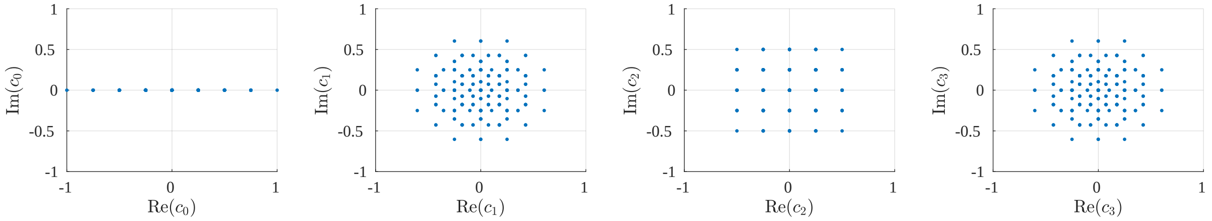

Figure 6: All possible values of the first four time-domain samples of an BPSK OFDM symbol with eight subcarriers. Odd samples are numerically diverse, i.e., contain a lot of information about the symbol sequence.

3.3.1 Direct demodulation. This approach feeds the early-detect signal with trailing zeros into an OFDM demodulator. This is equivalent to applying the FFT on the ideal symbol multiplied with a 1-0 step function. Doing so, the attacker directly maps the time-domain samples to all frequency subcarriers in order to then detect the bits. The shortcoming of this approach is that the ED condition (i.e., the later samples being cut off) is equivalent to applying a sharp filter in time domain, which corresponds to a wide (1/f) dispersion profile in frequency domain. This means every bit is subject to significant inter-carrier interference, which results in a relatively high bit error rate. The computational complexity of this approach is given by the FFT algorithm, i.e., $O(n_s \log(n_s))$.

3.3.2 Number-theoretic viewpoint. In this section, we deal with an idealized early-detection attacker that matches the observed time-domain samples against all possible symbols. Security against such an attacker can only be based on numerical ambiguity of the initial samples. However, as we will show, the initial samples of BPSK-modulated OFDM symbols contain a substantial amount of information about the entire sequence—a fact directly related to the FFT size being a power of two.

The set of possible time-domain values of each sample is limited, as we illustrate in Figure 6. The figures show the possible values that can be assumed by the first four time-domain samples for all possible bit sequences of a BPSK OFDM symbol with eight subcarriers. We can observe that the odd samples (i.e., samples c_1 and c_3) can assume many different distinct values because those are based on a linear combination of all distinct complex exponentials. Numerical matching exploits the systematic nature of the modulation, i.e., the fact that the limited frequency-domain constellation points, together with distinct complex exponentials, result in distinct numerical time-domain samples. By analyzing the conditions under which the numerical samples represent unique bit combinations, we can arrive at a concrete upper bound of the number of time-domain samples representing the bits of the symbol unambiguously.

Theorem 3.1. *An attacker with infinite sensitivity operating on a non-pulsed BPSK OFDM symbol*[2] *(with $n_s = 2^M$ for $M \in \mathbb{Z}^{>1}$) requires at most $n_s/4 + 1$ samples to detect the symbol.*

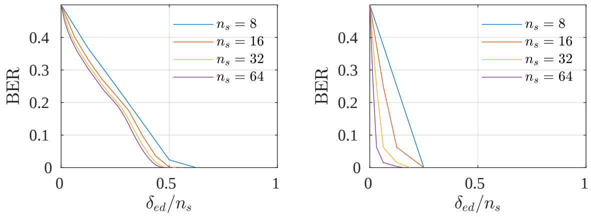

Figure 7: Early-detection bit error rate under direct demodulation (left) and ideal attacker behavior (right) as a function of the relative detection delay δ_{ed}/n_s.

The proof is provided in Appendix A. For BPSK, we show the resulting bit error rate as a function of the early-detection delay δ_{ed} in Figure 7, and contrast it to direct demodulation. Our bound indicates full symbol knowledge at sample $c_{n_s/4}$, whereas direct demodulation requires more than half the samples for error-free detection.

A brute-force attacker that matches time-domain samples against pre-computed traces faces a space complexity of $O\left(3^{n_s/2}\right)$. However, it is expected that polynomial-time maximum likelihood detectors exist. The fact that both the nature of the inter-carrier interference and the possible constellation points are known to the attacker makes a compelling case for the existence of efficient cancellation techniques.

Furthermore, we can reduce the problem of ideal time-domain matching in 4-QAM to the same problem on two interleaved BPSK symbols.

Corollary 3.2. *An attacker with infinite sensitivity operating on a non-pulsed 4-QAM OFDM symbol*[3] *requires at most $n_s/2 + 1$ samples to detect the symbol.*

Proof. Without loss of generality, an attacker can run the early-detection on the signal that is circularly shifted by $n_s/4$ to the left and start the early-detection procedure $n_s/4$ delayed. This is equivalent to a multiplication of the frequency-domain representation by a sequence $1, -i, -1, i, \ldots$. Starting with c_1, the attacker can then separate every sample of the shifted representation in its symmetric and antisymmetric components, which correspond to the time-domain representation of the real and imaginary parts of the frequency-domain symbols. These components are individually BPSK-modulated. Theorem 3.1 states that a non-pulsed BPSK

[2] As a non-pulsed BPSK symbol we define a symbol that under no (time-domain) circular shift has $\mathrm{C} = \pm\{1, 1, \ldots\}$

[3] As a non-pulsed 4-QAM symbol we define a symbol that under no (time-domain) circular shift has $\mathcal{R}(\mathrm{C}) = \pm\{1, 1, \ldots\}$ or $\mathcal{I}(\mathrm{C}) = \pm\{1, 1, \ldots\}$

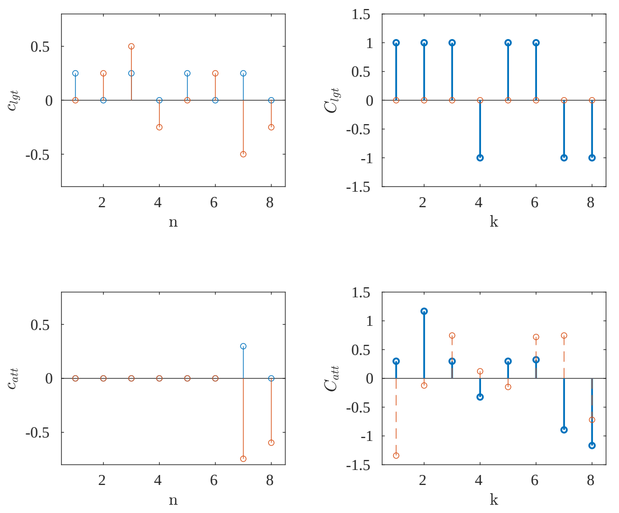

Figure 8: Example of a late-commit attack on BPSK OFDM. Ideal signal (top) vs. adversarial signal (bottom), both in time (left) and frequency domain (right). The attacker only provides the last two time-domain samples yet can create the correct BPSK symbol, as only the real part (blue) of the frequency-domain representation is of interest.

symbol requires at most $n_s/4 + 1$ samples for early-detection. Together with the offset required for the shift operation, we arrive at $n_s/4 + n_s/4 + 1 = n_s/2 + 1$ samples for ideal early-detection of the non-pulsed 4-QAM symbol. □

The same separation strategy for frequency-domain I and Q components can be applied irrespective of constellation density. Our main insight from the number-theoretic analysis is that, without assumptions on an attacker's sensitivity, even early samples contain a substantial amount of differential information about the entire symbol which, due to the structure of the constellation, directly translates to information about the symbol bits.

3.4 Late-commit

The late-commit problem for the attacker consists in finding a sequence of samples that result in the correct symbol at the receiver under a delayed onset of transmission. For a given symbol, the ability of an attacker to late-commit with a certain delay is not probabilistic but an immutable property of this symbol.

The fundamental principle behind late-committing to a symbol is reflected by the fact that the attacker does not have to provide a signal that is actually close on the physical layer (e.g., in the L2-sense), but only one that creates the correct bits at the receiver. In general, finding a valid late-commit sequence for an OFDM symbols is not straightforward. There is room for optimization on a per-symbol basis beyond just sending the late part of the symbol, as we illustrate in Figure 8.

Irrespective of the optimization technique, for a given symbol sequence $\mathbf{b}$ and transmission delay δ_{lc}, the goal of the attacker is to find a late-commit signal $\mathbf{c}^{lc}$ consisting of $n_s - \delta_{lc}$ samples that, if prepended with δ_{lc} zeros, minimizes the Hamming Distance $H(\, , \,)$ between the demodulated late-commit signal and the actual symbol sequence $\mathbf{b}$. The optimal late-commit algorithm LC is defined as

$$LC(\mathbf{b}, \delta_{lc}) = \underset{\mathbf{c}^{lc}}{\arg\min} \left\{ H\left(OFDM^{-1}\left(0^{\delta_{lc}} || \mathbf{c}^{lc}\right), \mathbf{b}\right)\right\}.$$

We say LC is a δ_{lc}-LC algorithm under symbol set $\mathcal{B}$ iff

$$H\left(OFDM^{-1}\left(0^{\delta_{lc}} || LC(\mathbf{b}, \delta_{lc})\right), \mathbf{b}\right) = 0, \forall \mathbf{b} \in \mathcal{B},$$

meaning an OFDM receiver will correctly interpret each symbol sequence despite the attacker omitting the first δ_{lc} samples of each time-domain symbol. A $\hat{\delta}_{lc}$-LC algorithm is optimal if there exists no δ_{lc}-LC algorithm for $\delta_{lc} < \hat{\delta}_{lc}$.

In the following, we will constructively prove the existence of a $n_s/2$-LC algorithm for the full BPSK symbol set without c_0-pulses, i.e. for $\mathcal{B}' = \mathcal{B} \setminus \mathcal{P}$, whereas $\mathcal{P} = \{\pm(1, 1, 1, ...)\}$.

3.4.1 Deterministic BPSK late-commit ($n_s/2$-LC). As a consequence of Hermitian symmetry, a late-committing attacker can generate any non-pulse BPSK symbol using only the samples corresponding to the second half of the symbol.

Theorem 3.3. *There exists a $n_s/2$-LC algorithm under the set of all non-pulsed BPSK OFDM symbols.*

The proof is provided in Appendix B. The critical observation behind the proof is that the attacker's first samples fully determines the amount of real-valued inter-carrier interference under the late-commit condition (i.e., the first $n_s/2$ samples being zero). A small decrease of this sample will decrease ICI more than the adverse effect its reduction has on the amplitude values, which are essential for correct BPSK detection.

3.4.2 4-QAM optimized late-commit. We can define an optimization problem that adjusts the time-domain sample in a way that maximizes the chances of correct detection, based on a frequency-domain metric (error function) that captures how close the signal is to the legitimate bit sequence. We choose an error function $\lambda\left(\, , \, \right)$ that punishes erroneous bits in proportion to the square norm of the deviation the from decision boundary. We provide the detailed definition of $\lambda\left(, \right)$ in Appendix C.

We then apply a gradient-descent optimization on the late-commit symbol subject to this error function.

I.e., for a symbol $\mathbf{b}$, choose $\mathbf{c}^{lc}$, s.t.

$$\lambda\left(MAP\left(\mathbf{b}\right), \mathcal{F}\left\{0^{\delta_{lc}} || \mathbf{c}^{lc}\right\}\right) \text{ minimal.}$$

We show the resulting bit-error rate under this optimization technique as a function of the late-commit delay δ_{lc} in Figure 9.

3.5 ED/LC attack

We have presented independent strategies for early-detection and late-commit. This section deals with how an attacker can combine these elements into a successful distance-reduction attack. This combination is characterized by a transition step from early-detection to late-commit. An ED/LC attack consists of independent stages for detection and late-commit, separated by the attacker's reduction target. We propose three fundamental strategies for transitioning from early-detection to late-commit. The first uses the

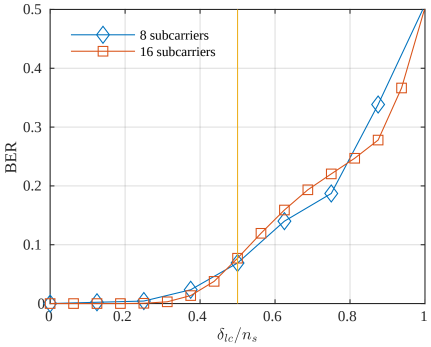

Figure 9: Adversarial BER under 4-QAM gradient-descent late-commit as a function of the relative late-commit delay. The vertical line marks the maximum early-detection delay of an ideal attacker.

same transition time for all symbols in the symbol set, the second chooses the transmission time adaptively, given the symbol. Thirdly we propose an adversarial strategy that is more general, without a strict transition.

3.5.1 Fixed transition. This attacker uses a fixed portion of each symbol for early-detection and late-commit. This corresponds to an attacker that does not pre-generate all late-commit signals in advance but generates the signal on the fly and transmits it at the earliest time required for any symbol in the symbol set. The latest late-commit time of any symbol in the message set will therefore be considered a strict upper bound for the delay at which the attacker has to guess the symbol under a given target for distance reduction.

The resulting adversarial advantage can be expressed in terms of the early-detection advantage, as

$$A(\mathcal{B}, \delta_{adv}) = A_{ED}\left(\mathcal{B}, \hat{\delta}_{lc}(\mathcal{B}) - \delta_{adv}\right),$$

for an advancement goal δ_{adv}.

3.5.2 Symbol-adaptive transition. This attacker incrementally learns about the symbol and uses this knowledge to optimize the start time of the late-commit attack. For this purpose, the attacker can be thought to maintain an uncertainty-set of symbols at each stage of the early-detection process and chooses the late-commit time to satisfy the lowest late-commit delay within this set. This way, the attacker optimizes the late-commit start time subject to his knowledge gained from early-detection. This behavior requires the attacker to pre-generate a significant fraction of all late-commit symbols in order to generate statistics on the latest possible late-commit delays subject to every symbol. The adversarial advantage under this model is bounded by the attacker's ability to correctly guess the symbol at the latest possible transmission time, given a certain reduction goal:

$$A(\mathcal{B}, \delta_{adv}) \leq \mathbb{E}_{\mathbf{b} \leftarrow \mathcal{B}}\left[A_{ED}\left(\mathbf{b}, \hat{\delta}_{lc}(\mathbf{b}) - \delta_{adv}\right)\right]$$

As an over-approximation of the attacker, we can consider above at equality. This corresponds to an attacker never waiting too long to start transmission of the late-commit symbol, i.e., being optimally informed about $\hat{\delta}_{lc}(\mathbf{b})$.

	n_s			
	8	**16**	**32**	**64**
$\delta_{lc} - \delta_{ed}$ at $A = 1$	1	3	7	15
$\Delta_t = (\delta_{lc} - \delta_{ed})(n_s/20MHz)$	50ns	150ns	350ns	750ns
$\Delta_d = \Delta_t * c$	15m	45m	105m	225m

Table 1: Maximum time advancement for BPSK OFDM at adversarial advantage $A = 1$, using ideal early-detection and a fixed transition. We assume a total bandwidth of 20MHz split into varying numbers of subcarriers.

3.5.3 Interleaved ED/LC. This is the most generalized model with regards to the attacker's transition from ED to LC. It assumes the attacker continuous detects the legitimate symbol, even after starting to transmit late-commit samples. In other terms, this is an attacker that might start transmitting before getting a clear picture from the early-detection, and adjust each transmitted samples to new observations. This corresponds to the attacker model put forward in [16].

3.6 Distance reduction attack

We evaluate the vulnerability of BPSK and 4-QAM OFDM to an ED/LC distance-reduction attack by combining our findings for early-detection and late-commit.

3.6.1 BPSK. BPSK OFDM is vulnerable to an ED/LC attack that results in a deterministically successful distance reduction by a physical-layer attacker under the fixed transition model. We have proven that the attacker requires only half the samples for successful late-commit and a quarter of the samples for early-detection. This means the attack succeeds irrespective of asymptotic properties on the bit- and frame level (i.e., independently of the quality of entropy of the message bits and how many messages are exchanged).

Corollary 3.4. *An (ideal) attacker operating on a non-pulsed BPSK OFDM symbol can achieve a distance reduction corresponding to up to $n_s/4 - 1$ samples deterministically.*

Proof. Theorem 3.3 states that for any non-pulsed BPSK OFDM symbol, there exists an $n_s/2$-*LC* algorithm. Theorem 3.1 states that an attacker requires up to $n_s/4 + 1$ samples to detect a non-pulsed BPSK OFDM symbol ideally. This leaves an attacker with $n_s/2 - (n_s/4 + 1) = n_s/4 - 1$ samples for distance reduction with $A = 1$ under the fixed transition model. □

Table 1 exemplifies the impact of the sample-level advancement on time and distance. For the numerical example, we assume a system bandwidth of 20MHz, split into various numbers of subcarriers. The sample spacing is determined as the inverse of the system bandwidth. We observe a higher impact for systems with more and narrower subcarriers, e.g., the typical configuration for an IEEE 802.11 system consisting of 64 subcarriers is vulnerable to a distance reduction of up to 225m if BPSK is used. It becomes evident that, under a fixed system bandwidth, higher numbers of subcarriers come at a loss for secure ToF measurement due to the fact that the symbol duration is increased.

3.6.2 4-QAM. Corollary 3.2 states that an attacker requires only $n_s/2+1$ samples to ideally detect a 4-QAM symbol. The late-commit profile shown in Figure 9 shows that a late-committing attacker achieves a BER of below 10% at the half-symbol mark. Together this indicates that a significant adversarial advantage remains for performing a distance-reduction attack, even under the fixed-transition model. Because the learning curve for early-detection is steep, i.e., the sample with index $n_s/4 + 3$ already reveals more than 90% of the symbol information, there is also a potential for an interleaved strategy, which would likely further reduce the adversarial bit-error-rate.

4 CAN OFDM BE SECURED?

After identifying the major problems with secure ranging based on OFDM, this section proposes a potential direction for securing OFDM-based ranging. The underlying observation is that the possible set of constellation points can be randomized and extended to cover a continuous disk in the IQ plane, minimizing an adversary's structural knowledge about the modulation.

4.1 Continuous extension of constellation

We can increase the constellation density on the transmit-side by limiting the modulation to one dimension and adding a *noise dimension* to each tone. The rationale is to increase the numerical diversity of the resulting time-domain samples.

In addition, we can add a random phase shift to each tone that is pre-shared and inverted by the receiver before demodulation. Phase randomization is a common technique for PAPR reduction, i.e., existing hardware is expected to implement it. This approach leverages the same procedure for security against early detection. The random phase offsets create a dense, concentric constellation pattern if jointly applied with orthogonal noise and a denser than minimal constellation set (e.g., eight constellation points in the information dimension). If we move beyond BPSK for the information dimension, the resulting frequency-domain constellation covers a concentric disk. We can choose orthogonal noise and phase offset at an arbitrarily fine resolution without any impact on performance. This leaves an attacker with minimal a-priori numerical knowledge, only a lower and upper bound on each tone's amplitude.

4.2 Evaluation

We analyze our proposal, consisting of eight constellation points in the information dimension, together with orthogonal noise and phase randomization, in terms of its security against early-detection.

4.2.1 Information-theoretic security against ED. Phase randomization together with fine-grained orthogonal noise can provide information-theoretic security against an early-detecting attacker. The fundamental reason that any point in a continuous area in the IQ-plane is a valid value for each frequency-domain sample. This means, any partial time-domain sequence can be continued in many ways such that each tone ends up within the valid range. This uncertainty is associated with a certain bit error rate. We verified this in a simulation, where we randomly sampled valid continuation (vc) sequences for many different symbols and evaluated their resulting bit-error rate, as shown in Figure 10. We contrast them to zero-extended (zc) symbols and see no difference in the resulting bit error rate.

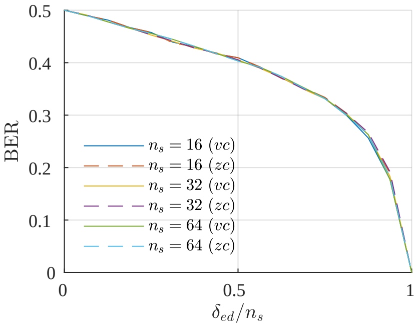

Figure 10: Bit-error rate of an early-detecting attacker against full phase-randomization with orthogonal noise as a function of the relative detection delay and for different numbers of subcarriers.

5 DISCUSSION

In the following, we cover the main avenues that can be taken to secure OFDM signals against an ED/LC attacker and highlight a few additional OFDM features that are linked to physical-layer security.

5.1 Preventing LC: ICI sensitivity

Late-commit detection is enabled by a receiver's ability to detect deviations from the expected signal shape.

5.1.1 Utilizing both signal-space dimensions. Utilizing both signal-space dimensions in frequency domain breaks up the symmetry of the time-domain signal around symbol center and is, therefore, a necessity against both early-detection and late-commit.

5.1.2 Denser Constellation. Late-commit attacks become less effective if information is modulated on a denser constellation grid. As a consequence, late-commit needs to start earlier, as inter-carrier-interference has more impact. The denser the constellation, the less dispersion can be tolerated for correct detection. In general, denser constellations and increased throughput come at a tension with robustness, a requirement which is especially important since cyclic prefix and channel compensation cannot be used for security reasons.

5.1.3 Error integration. A possible way to resolve this tension is to map the signal into a denser constellation at the receiver and then post-process the received bits in a way that approximates the L2 distance to the expected spectrum (and selecting an appropriate symbol-wide decision threshold). This way, significant deviations of only a few tones can be weighted accordingly, and late-commit strategies that optimize for low bit-error rate under a coarse constellation mapping lose their utility.

5.2 Secure time-domain signals over OFDM

Due to inherent drawbacks of OFDM for secure ranging, i.e., the countermeasure requiring additional power for a noise dimension, and significant shared entropy for phase correction, it might be of use to retrofit OFDM transceivers with time-domain modulation capability. One such proposal is the use of DFT-spread OFDM. Outside of OFDMA, this just means to precode the IQ values as spectrum of a time-domain signal. This results in similar properties of the signal to any time-domain pulsed modulation.

A way to create secure time-domain signals without need for additional DFT blocks is to transmit a single pulse per symbol, as in [24]. This can be achieved by using identical tones (of a certain polarity) and verifying correctness either by a time-domain technique or, alternatively, evaluating the Hamming weight per symbol at the receiver (serving as approximation for the polarity of a constrained pulse in time-domain). The drawback of this approach is its data rate, i.e., one symbol can only transmit one bit and a longer series of ranging symbols has to be exchanged.

5.3 Other aspects

Different mechanisms that are commonly used for enhancing performance of OFDM systems can have a detrimental impact on physical-layer security.

5.3.1 Channel sensing and equalization. A secure ranging implementation based on OFDM cannot rely on channel sensing and equalization. Channel sensing can be manipulated by an attacker, which brings equalization under adversarial control. Fundamentally, channel compensation is about compensation of time-dispersion, which leads delayed signal components being included in the decoding.

5.3.2 Cyclic prefix. The cyclic prefix, commonly applied on OFDM symbols to achieve orthogonal equalization under a channel, should not be used in symbols used for secure ranging, as it provides an additional advantage to the early-detecting adversary. The rationale behind the cyclic prefix is to prepend the trailing samples of the symbol at its beginning and, in turn, to circularize the Fourier matrix under a time-dispersive channel. This creates symbol redundancy which helps an early-detecting attacker.

5.3.3 PAPR reduction techniques. Orthogonal noise with a random phase shift is compatible with techniques for peak-to-average power reduction, as phase randomization is one of those techniques. Another technique for PAPR reduction is to reduce the symbol set to low-PAPR symbols. With BPSK and QPSK, pruning the symbol set of high-PAPR symbols tends to remove symbols with very stringent late-commit constraints, which might add to the overall vulnerability of those configurations.

6 RELATED WORK

We compare our analysis of multicarrier-based ranging with existing proposals for secure single-carrier ranging, as well as other physical-layer concepts in wireless communication. In particular, we focus on mechanisms that attempt to protect a wireless signal on the physical layer. Secure ranging achieves a similar goal since it has to guarantee that the arrival time of the signal can not be subverted by external influence, in addition to the protection of physical layer attributes and data integrity.

6.1 Single-carrier Ranging

Research has yielded a handful of protocols for secure single-carrier ranging and distance measurements. The majority of them focus on ultrawide-band radio (UWB), a technology that provides non-cooperative communication at bandwidths of up to 500 MHz. Due to their wide spectral use, UWB devices have to operate at limited output power, but the high bandwidth allows them to send short pulses that have high immunity to multi-path fading. If data is encapsulated in nano-second pulses, the surface for ED/LC attacks is very narrow since an attacker is forced to advance or delay single pulses. Different effective proposals that describe how pulses need to be emitted can be found in [16, 23].

The UWB technology has also resulted in few commercial products [1, 2]. However, the main disadvantage of UWB ranging is its limited power output and as a consequence, distances greater than 50 to 100 meters (depending on channel conditions) are difficult to overcome. As a remedy, frame size has to be increased, but this leads to long communication times in an already uncoordinated spectrum. UWB ranging is therefore mainly used for indoor positioning or in two-device configurations, such as key-less entry systems for vehicles.

OFDM, on the other hand, has proven to be an extremely reliable modulation technique. While techniques for improving the performance of OFDM-based ranging have been proposed [12], its security against physical-layer attacks has, to the best of our knowledge, not been studied so far. OFDM-based communication systems can cover distances on the order of kilometers and coordinate many co-existing devices, such as in 4G and the new 5G standard. On the downside, symbol length for OFDM-encoded data is generally longer than UWB pulses—an important reason to study the security of OFDM systems when used for ranging.

6.2 Physical-Layer Integrity Protection Schemes and Jamming

There exist many physical-layer schemes that aim to guarantee the integrity of transmitted data. They can roughly be divided into randomness extraction from the channel (key establishment), MIMO-based approaches (orthogonal blinding, zero-forcing), friendly jamming and integrity codes [28].

The concept of friendly jamming is related to the countermeasures for OFDM-based ranging that we propose in this work. The idea behind phase randomization and orthogonal noise is similar to that of friendly jamming [9, 20] where an attacker can not separate the information-bearing message from a jamming signal emitted by a friendly jammer. The concept of intentional signal interference can be used to establish confidentiality, message authentication or access control [13, 26]. Reactive jamming on the other hand tries to analyze and react to packets in the air [7] in order to annihilate/overwrite certain packets or prevent communication altogether. This is related to the problem statement of the ED/LC attack described in this paper. In reactive jamming, it is crucial to detect a signal very early on, i.e., only based on parts of it, to have maximum impact when interfering with the remainder of the signal.

Probably most related to our work is the survey in [17] that compares different approaches to physical-layer security in OFDM. Most of the presented methods are concerned with confidentiality either on the data bits or on the symbol level. The main idea is to encrypt or obfuscate the signal and/or provide resiliency against interference [22]. The idea we present in this paper is similar in the sense that an attacker should not be able to predict the transmitted signal. However, we propose secure ranging schemes that protect the communication on the symbol level, rather than entire messages. Furthermore, we are specifically concerned with the learning/listening time that an attacker requires until the remainder of the symbol can be predicted since this is the crucial factor that facilitates secure time-of-flight ranging.

7 CONCLUSION

We highlighted the vulnerability of highly performant OFDM modulation schemes for ToF distance measurement against an ED/LC attacker operating on the physical layer. Existing proposals for secure ToF distance measurement developed for single-carrier modulation methods require time-domain focusing of bit-information (pulsing) and time-domain padding. This work identified another possible direction suited to OFDM systems, using all subcarriers in parallel with randomized constellations.

ACKNOWLEDGMENTS

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program under grant agreement No 726227.

REFERENCES

[1] [n.d.]. 3db Access AG - Proximity based access control. https://www.3db-access.com/. [Online; Accessed March 25th 2021].

[2] [n.d.]. DW1000 Radio IC - Decawave. https://www.decawave.com/product/dw1000-radio-ic/. [Online; Accessed March 25th 2021].

[3] Task Group 4z. [n.d.]. IEEE 802.15 WPAN "Enhanced Impulse Radio". http://www.ieee802.org/15/pub/TG4z.html. [Online; Accessed March 25th 2021].

[4] Gildas Avoine, Muhammed Ali Bingöl, Ioana Boureanu, Srdjan čapkun, Gerhard Hancke, Süleyman Kardaş, Chong Hee Kim, Cédric Lauradoux, Benjamin Martin, Jorge Munilla, Alberto Peinado, Kasper Bonne Rasmussen, Dave Singelée, Aslan Tchamkerten, Rolando Trujillo-Rasua, and Serge Vaudenay. 2018. Security of Distance-Bounding: A Survey. *ACM Comput. Surv.* 51, 5, Article 94 (Sept. 2018), 33 pages.

[5] Task Group az. [n.d.]. IEEE 802.11 "Next Generation Positioning". http://www.ieee802.org/11/Reports/tgaz_update.htm. [Online; Accessed 25. March 2021].

[6] Task Group az. [n.d.]. Versioning for PHY Security. https://mentor.ieee.org/802.11/dcn/20/11-20-1972-01-00az-versioning-of-phy-security.pptx. [Online; Accessed 25. March 2021].

[7] Daniel S. Berger, Francesco Gringoli, Nicolò Facchi, Ivan Martinovic, and Jens Schmitt. 2014. Gaining Insight on Friendly Jamming in a Real-World IEEE 802.11 Network. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Oxford, United Kingdom) *(WiSec '14)*. Association for Computing Machinery, New York, NY, USA, 105–116. https://doi.org/10.1145/2627393.2627403

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

[9] Bhaswati Deka, Ryan M. Gerdes, Ming Li, and Kevin Heaslip. 2015. Friendly Jamming for Secure Localization in Vehicular Transportation. In *International Conference on Security and Privacy in Communication Networks*, Jing Tian, Jiwu Jing, and Mudhakar Srivatsa (Eds.). Springer International Publishing, Cham, 212–221.

[10] Manuel Flury, Marcin Poturalski, Panos Papadimitratos, Jean-Pierre Hubaux, and Jean-Yves Le Boudec. 2010. Effectiveness of Distance-decreasing Attacks Against Impulse Radio Ranging. In *Proceedings of the Third ACM Conference on Wireless Network Security* (Hoboken, New Jersey, USA) *(WiSec '10)*. ACM, New York, NY, USA, 117–128. https://doi.org/10.1145/1741866.1741887

[11] Stuart A Golden and Steve S Bateman. 2007. Sensor measurements for Wi-Fi location with emphasis on time-of-arrival ranging. *IEEE Transactions on Mobile Computing* 6, 10 (2007).

[12] Azadeh Haghparast, Traian Abrudan, and Visa Koivunen. 2009. OFDM ranging in multipath channels using time reversal method. In *2009 IEEE 10th Workshop on Signal Processing Advances in Wireless Communications*. 568–572. https://doi.org/10.1109/SPAWC.2009.5161849

[13] J. Kim and J. P. Choi. 2016. Cancellation-Based Friendly Jamming for Physical Layer Security. In *2016 IEEE Global Communications Conference (GLOBECOM)*. 1–6. https://doi.org/10.1109/GLOCOM.2016.7841646

[14] Manikanta Kotaru, Kiran Joshi, Dinesh Bharadia, and Sachin Katti. 2015. Spotfi: Decimeter level localization using wifi. In *ACM SIGCOMM Computer Communication Review*, Vol. 45. ACM, 269–282.

[15] Tsit Yuen Lam and Ka Hin Leung. 2000. On vanishing sums of roots of unity. *Journal of algebra* 224, 1 (2000), 91–109.

[16] Patrick Leu, Mridula Singh, Marc Roeschlin, Kenneth G. Paterson, and Srdjan Capkun. 2020. Message Time of Arrival Codes: A Fundamental Primitive for Secure Distance Measurement. In *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*. IEEE, 500–516. https://doi.org/10.1109/SP40000.2020.00010

[17] Reem Melki, Hassan N. Noura, Mohammad M. Mansour, and Ali Chehab. 2019. A survey on OFDM physical layer security. *Physical Communication* 32 (2019), 1 – 30. https://doi.org/10.1016/j.phycom.2018.10.008

[18] Andreas F Molisch. 2012. *Wireless communications*. Vol. 34. John Wiley & Sons.

[19] M. Poturalski, M. Flury, P. Papadimitratos, J. P. Hubaux, and J. Y. Le Boudec. 2011. Distance Bounding with IEEE 802.15.4a: Attacks and Countermeasures. *IEEE Transactions on Wireless Communications* 10, 4 (April 2011), 1334–1344. https://doi.org/10.1109/TWC.2011.020111.101219

[20] Hanif Rahbari and Marwan Krunz. 2014. Friendly CryptoJam: A Mechanism for Securing Physical-Layer Attributes. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless and Mobile Networks* (Oxford, United Kingdom) *(WiSec '14)*. Association for Computing Machinery, New York, NY, USA, 129–140. https://doi.org/10.1145/2627393.2627415

[21] A. Ranganathan and S. Capkun. 2017. Are We Really Close? Verifying Proximity in Wireless Systems. *IEEE Security Privacy* 15, 3 (2017), 52–58.

[22] C. Shahriar, M. La Pan, M. Lichtman, T. C. Clancy, R. McGwier, R. Tandon, S. Sodagari, and J. H. Reed. 2015. PHY-Layer Resiliency in OFDM Communications: A Tutorial. *IEEE Communications Surveys Tutorials* 17, 1 (Firstquarter 2015), 292–314. https://doi.org/10.1109/COMST.2014.2349883

[23] Mridula Singh, Patrick Leu, and Srdjan Capkun. 2019. UWB with Pulse Reordering: Securing Ranging against Relay and Physical-Layer Attacks. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society. https://www.ndss-symposium.org/ndss-paper/uwb-with-pulse-reordering-securing-ranging-against-relay-and-physical-layer-attacks/

[24] Mridula Singh, Marc Röschlin, Aanjhan Ranganathan, and Srdjan Capkun. 2020. V-Range: Enabling Secure Ranging in 5G Wireless Networks. (2020).

[25] Nils Ole Tippenhauer, Heinrich Luecken, Marc Kuhn, and Srdjan Capkun. 2015. UWB rapid-bit-exchange system for distance bounding. In *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2.

[26] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun. 2013. On Limitations of Friendly Jamming for Confidentiality. In *2013 IEEE Symposium on Security and Privacy*. 160–173. https://doi.org/10.1109/SP.2013.21

[27] Deepak Vasisht, Swarun Kumar, and Dina Katabi. 2016. Decimeter-Level Localization with a Single WiFi Access Point.. In *NSDI*, Vol. 16. 165–178.

[28] S. Čapkun, M. Čagalj, R. Rengaswamy, I. Tsigkogiannis, J. Hubaux, and M. Srivastava. 2008. Integrity Codes: Message Integrity Protection and Authentication over Insecure Channels. *IEEE Transactions on Dependable and Secure Computing* 5, 4 (2008), 208–223. https://doi.org/10.1109/TDSC.2008.11

A BPSK EARLY DETECTION

Proof. An OFDM time-domain sample can be represented as the IFFT of the frequency-domain modulated symbol samples. In the following, we will show that left-right antivalent bits (i.e., bits that do not repeat after $n_s/2$ samples) are leaked with the first odd (respectively, any odd) sample. For the first odd sample, we have

$$c_1 = \sum_{k=0}^{n_s-1} C_k e^{2\pi i k/n_s}$$

$$= \sum_{k=0}^{n_s/2-1} C_k e^{2\pi i k/n_s} + \sum_{k=n_s/2}^{n_s-1} C_k e^{2\pi i k/n_s}$$

$$= \sum_{k=0}^{n_s/2-1} \left(C_k + e^{\frac{2\pi i n_s/2}{n_s}} C_{k+n_s/2} \right) e^{2\pi i k/n_s}$$

$$= \sum_{k=0}^{n_s/2-1} (C_k - C_{k+n_s/2}) e^{2\pi i l k/n_s},$$

since

$$e^{\frac{2\pi i n_s/2}{n_s}} = e^{\pi i} = -1.$$

Due to the limited constellation set of BPSK modulation (i.e., $C_k \in \{-1, 1\}$), we can express the difference between frequency-domain samples in terms of a logical bit-level operation:

$$c_1 = 2 \sum_{k=0}^{n_s/2-1} C_k (b_k \oplus b_{k+n_s/2}) e^{2\pi i k/n_s}$$

The negative sign is equivalent to a π-phase rotation of the complex exponential, therefore, equivalently:

$$c_1 = 2 \sum_{k=0}^{n_s-1} a_k e^{2\pi i k/n_s}, \ a_k \in \{0, 1\}$$

In order to understand whether c_1 uniquely represents the sequence a, we consider the difference between two of these polynomials for different sequences $a^{(1)}$ and $a^{(2)}$:

$$\sum_{k=0}^{n_s-1} a_k^{(1)} e^{2\pi i k/n_s} - \sum_{k=0}^{n_s-1} a_k^{(2)} e^{2\pi i k/n_s}, \ a_k^{(1)}, a_k^{(2)} \in \{0, 1\}$$

$$= \sum_{k=0}^{n_s-1} \varepsilon_k e^{2\pi i k/n_s}, \ \varepsilon_k \in \{0, 1, 2\}$$

We assume the sequences $a^{(1)}$ and $a^{(2)}$ not to be identical, therefore there exists a $k \in \{0, ..., n_s - 1\}$, for which $\varepsilon_k > 0$. Therefore, this is a sum over up to $n_s/2$ of the n_s-th roots of unity, with $\varepsilon_k \varepsilon_{k+n_s/2} = 0$. For the sake of contradiction, we consider the above expression to be zero, i.e.,

$$\sum_{k=0}^{n_s-1} \varepsilon_k e^{2\pi i l k/n_s} = 0, \ \varepsilon_k \in \{0, 1, 2\}.$$

A result from algebraic number theory reveals interesting properties of such vanishing sums of roots of unity [15]. Corollary 3.4 in [15] states that if $m = p^a q^b$, where p, q are primes, then, up to a rotation, the only minimal vanishing sums of m-th roots of unity are $1 + \zeta_p + ... + \zeta_p^{p-1}$ and $1 + \zeta_q + ... + \zeta_q^{q-1}$ (where ζ_p denotes a p-th primitive root of unity), and rotations thereof. A minimal vanishing sum is defined as a sum of roots of unity that amounts to zero, yet contains no sub-sum that is zero. In our case, due to the FFT size being a power of two, we have $p = q = 2$, meaning the only minimal vanishing sum is given by one plus the 2nd primitive root of unity (and rotations thereof). This means, $1 - 1$, and rotations thereof, i.e., $e^{\rho i} + e^{(\rho + \pi)i}$ for $\rho \in [0, \pi)$. However, since we have $\varepsilon_k \varepsilon_{k+n_s/2} = 0$, the expression above does a) not contain any minimal vanishing sum nor b) constitute a minimal vanishing sum, which proves the contradiction.

In consequence, every left-right antivalence in the bit sequence results in a unique contribution to every odd time-domain sample. Left-right equialence, on the other hand, cancels out the contributions. This means, the odd sample does not convey any information on bits that repeat after $n_s/2$ samples, however, conveys all information about bits that are inverted after $n_s/2$ samples. Conversely, the first non-zero even sample (i.e., the sample c_2) is oblivious to information about tones that repeat after $n_s/4$ samples, however conveys information about antivalence of tones $n_s/4$ apart.

In the following, we consider the sequence of samples with indices that are powers of two ($l = 2^L$ and $0 \leq L < M$).

From sample c_1, we learn the sequence $C_k(b_k \oplus b_{k+n_s/2})$, i.e., the values of the left-right antisymmetric bits. We can create a compensation term $\sum_{k=0}^{n_s/2-1} C_k(b_k \oplus b_{k+n_s/2}) e^{2\pi i 2k/n_s}$ and add it to c_2, which recovers the equivalent sample of the IFFT on the first half of the spectrum only, since

$$c_2 = \sum_{k=0}^{n_s-1} C_k e^{2\pi i 2k/n_s}$$

$$= \sum_{k=0}^{n_s/2-1} \left(C_k + e^{\frac{2\pi i 2 n_s/2}{n_s}} C_{k+n_s/2} \right) e^{2\pi i 2k/n_s}$$

$$= \sum_{k=0}^{n_s/2-1} \left(C_k + C_{k+n_s/2} \right) e^{2\pi i 2k/n_s}.$$

Hence,

$$c_2 + 2 \sum_{k=0}^{n_s/2-1} C_k (b_k \oplus b_{k+n_s/2}) e^{2\pi i 2k/n_s} = 2 \sum_{k=0}^{n_s/2-1} C_k e^{2\pi i 2k/n_s}$$

This allows, in turn, to recover the sequence $C_k(b_k \oplus b_{k+n_s/4})$ and so on.

This procedure can be invoked recursively until the sequence consists of four samples only. The remaining uncertainty is only given by the center pulse (i.e., 1,-1,1,-1 vs. -1,1,-1,1) (single equivalence is leaked by DC sample), which we exclude from the proof. Hence, under the last recursion step we have $n_s/2l = 2 \Leftrightarrow l = n_s/4$. This means, we need in total $n_s/4 + 1$ samples for ideal detection. □

B DETERMINISTIC BPSK LATE COMMIT

Proof. Consider a split of the frequency-domain symbol $\mathbf{C}$ into its even and odd contributions, i.e.,

$$C_k^{(E)} := C_{2k}, \ k = 0, ..., n_s/2 - 1,$$

$$C_k^{(O)} := C_{2k+1}, \ k = 0, ..., n_s/2 - 1.$$

The corresponding time-domain contributions are given by the inverse Fourier transform:

$$\mathbf{c}^{(E)} = \mathcal{F}^{-1} \left\{ \mathbf{C}^{(E)} \right\}$$

$$\mathbf{c}^{(O)} = \mathcal{F}^{-1} \left\{ \mathbf{C}^{(O)} \right\}$$

From the definition of the DFT, we know that

$$c_n = c_n^{(E)} + e^{-\frac{2\pi i}{n_s} n} \cdot c_n^{(O)}, \ n = 0, ..., n_s/2 - 1.$$

Hence, the late-commit condition, i.e.,

$$c_n = 0, \text{ for } n = 0, ..., n_s/2 - 1,$$

imposes a clear relationship between even and odd frequency-domain samples (as given by the trigonometric interpolation of every second sample), respectively, its individual time-domain contributions, i.e.,

$$c_n^{(E)} = -e^{-\frac{2\pi i}{n_s}n} \cdot c_n^{(O)} = -g_n \cdot c_n^{(O)}, \tag{1}$$

where we define the half-period complex exponential $\mathbf{g}$ as

$$g_n = e^{-\frac{2\pi i}{n_s}n},\ n = 0, ..., n_s/2 - 1.$$

Taking the Fourier transform of Equation 1 yields

$$\mathbf{C}^{(E)} = -\frac{1}{n_s}\mathbf{G} * \mathbf{C}^{(O)}, \tag{2}$$

where $\mathbf{G}$ is defined as

$$G_k = \sum_{n=0}^{n_s/2-1} e^{-\frac{i2\pi}{n_s}n} e^{-\frac{i2\pi}{n_s/2}nk} = \sum_{n=0}^{n_s/2-1} e^{-\frac{i2\pi}{n_s}n(1-2k)} \tag{3}$$

and can be considered a frequency-domain 'filter' that corresponds to said time-domain relationship, representing the resulting dispersion profile through inter-carrier interference. Importantly, the real part of Equation 3 constantly evaluates to 1, due to circular symmetry.

In the following, we treat the late-commit signal as a sum of the perfect odd and even contributions separately. Without loss of generality, we assume the odd contributions as ideal.

Only the real part of Equation 2 matters for BPSK symbols, for which the circular convolution evaluates to

$$\mathbb{R}\left\{\tilde{\mathbf{C}}^{(E)}\right\} = \mathbb{R}\left\{\mathbf{G}\right\} * \mathbf{C}^{(O)} = -\frac{1}{n_s}\sum_{k=0}^{n_s/2-1} C_k^{(O)}.$$

This follows from odd contributions being ideal, i.e. real values +1,-1 only, which means that only the real part of $\mathbf{G}$ matters.

Inter-carrier interference terms are given by respective first time-domain samples, for contribution with odd samples ideal:

$$\mathbb{R}\left\{\tilde{C_k}^{(E)}\right\} = -c_0^{(O)},$$

and for the contribution with even samples ideal:

$$\mathbb{R}\left\{\tilde{C_k}^{(O)}\right\} = -c_0^{(E)}$$

If we now assume the two contributions are added, we can imagine the value of every bit to contain an ideal contribution and an interference term. Correct detection is achieved if no bit is flipped due to the interference term. We, therefore, need to limit the inter-carrier-interference to be less than the legitimate signal value. Consider the superposition, where $c_0^{(O)\prime} = \alpha \cdot c_0^{(O)}$ and $c_0^{(E)\prime} = \alpha \cdot c_0^{(E)}$, for $\alpha \in (0, 1)$. This corresponds to a dampening of the first signal sample sent by the attacker by real-valued constant α. The resulting interference term will amount to $\alpha \cdot c_0^{(O)}$. The amplitude will be less affected, i.e., $1 \pm (1 - \alpha) \cdot c_0^{(E)}$. Without loss of generality (due to symmetry), we assume the bit to be 1. For correct detection of each bit, we need to have

$$\underbrace{1 - (1 - \alpha) \cdot c_0^{(E)}}_{Amplitude} - \underbrace{\alpha \cdot c_0^{(O)}}_{ICI} \overset{!}{>} 0$$

For $\alpha > 0$, this is equivalent to

$$c_0^{(E)} - c_0^{(O)} \overset{!}{>} \frac{c_0^{(E)} - 1}{\alpha},$$

which holds iff $\mathbf{c}$ is not a pulse (since 1 is maximum DC), and the condition is not satisfied iff both even and odd frequency samples have full DC, which corresponds to the spectral profile of a pulse. □

C 4-QAM OPTIMIZED LATE COMMIT

We define our error function as

$$\lambda\left(\mathrm{C}, \mathrm{C}^{lc}\right) = \sum_{n=0}^{n_S-1} \lambda_{\mathcal{R}}\left(C_n, C_n^{lc}\right) + \sum_{n=0}^{n_S-1} \lambda_{\mathcal{I}}\left(C_n, C_n^{lc}\right),$$

where

$$\lambda_{\mathcal{R}}\left(C_n, C_n^{lc}\right) = \begin{cases} 0, & |\mathcal{R}\left(C_n\right) - \mathcal{R}\left(C_n^{lc}\right)| \leq 1 \\ \left(\mathcal{R}\left(C_n\right) - \mathcal{R}\left(C_n^{lc}\right)\right)^2, & \text{otherwise} \end{cases}$$

and

$$\lambda_{\mathcal{I}}\left(C_n, C_n^{lc}\right) = \begin{cases} 0, & |\mathcal{I}\left(C_n\right) - \mathcal{I}\left(C_n^{lc}\right)| \leq 1 \\ \left(\mathcal{I}\left(C_n\right) - \mathcal{I}\left(C_n^{lc}\right)\right)^2, & \text{otherwise} \end{cases}$$