ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Analysis of OFDM-Based Ranging against Early-Detect/Late-Commit (ED/LC) Attacks

Semester Project

Raphaël Flückiger

Wednesday 11th February, 2026

Supervisor: Claudio Anliker, claudio.anliker@inf.ethz.ch
System Security Group, ETH Zürich

Abstract

Orthogonal Frequency Division Multiplexing (OFDM) is widely used in standards such as Wi-Fi, LTE, and 5G due to its efficiency and robustness. Beyond data transmission, secure ranging using OFDM waveforms allows for applications like passive keyless entry and start (PKES) systems. However, poor parameter choices can result in predictable symbols, making them susceptible to Early-Detect/Late-Commit (ED/LC) attacks. In such attacks, an adversary detects symbols early and injects signals to reduce the measured distance between devices.

This project investigates how OFDM parameters—specifically modulation order, number of subcarriers, and symbol length—affect susceptibility to ED/LC attacks in Wi-Fi ranging (IEEE 802.11az). We model OFDM transmission and attacker strategies to analyze the trade-off between attack success rate and complexity. We also explore AI-based early detection strategies and compare them with traditional methods.

Contents

Chapter 1

Introduction

1.1 Motivation

Orthogonal Frequency Division Multiplexing (OFDM) is the backbone of modern wireless communication, including Wi-Fi (IEEE 802.11). With the introduction of IEEE 802.11az, Wi-Fi now supports Fine Timing Measurements (FTM) for secure ranging. Secure ranging is critical for applications like access control (e.g., Passive Keyless Entry and Start systems) and secure payments. However, the physical properties of OFDM waveforms can introduce vulnerabilities if not carefully configured.

1.2 Problem Statement

Secure ranging relies on the integrity of the time-of-flight measurement. In an Early-Detect/Late-Commit (ED/LC) attack, an adversary infers the content of an OFDM symbol before it is fully received (Early Detect) and injects a malicious signal to alter the timestamp (Late Commit), effectively reducing the measured distance. This project attemps to reproduce IEEE task force analysis's on how OFDM parameters such as modulation order and symbol length influence the feasibility and success rate of these attacks.

1.3 Contributions

In this project, we:

- Analyze the theoretical susceptibility of OFDM waveforms to ED/LC attacks.
- Simulate OFDM transmission and multiple attacker strategies in Matlab/Python.

- Investigate the trade-off between attack success probability and computational complexity.
- Explore AI-based approaches for early symbol detection (though traditional methods remain the primary focus).

1.4 Thesis Organization

The remainder of this thesis is organized as follows: Chapter 2 provides background on OFDM and ranging security. Chapter 3 defines the system and threat models. Chapter 4 details the simulation environment and attack implementations. Chapter 5 presents the experimental results, and Chapter 6 concludes the work.

Chapter 2

Background

This chapter provides the necessary background on Orthogonal Frequency Division Multiplexing (OFDM), the principles of secure ranging, and the mechanics of Early-Detect/Late-Commit (ED/LC) attacks.

2.1 Orthogonal Frequency Division Multiplexing (OFDM)

Orthogonal Frequency Division Multiplexing (OFDM) is a multi-carrier modulation scheme that divides a high-data-rate stream into multiple lower-rate streams, which are transmitted in parallel over orthogonal subcarriers. This orthogonality allows for efficient spectrum usage and robust performance in multipath environments. OFDM is used in many communication schemes such as WiFi, LTE and 5G, mostly for high rate transmissions. For ranging purposes, as we will se later on, the requirements are different than those of data streams.

2.1.1 Modulation Mapping

The transmission process begins by mapping binary data bits onto complex-valued constellation symbols (usually they are represented in the IQ-plane). Let $\mathbf{X} = [X_0, X_1, \ldots, X_{N-1}]^T$ be the vector of frequency-domain symbols, where N is the total number of subcarriers. Each element X_k belongs to a specific modulation alphabet $\mathcal{M}$ (e.g., BPSK, QPSK, M-QAM). The choice of $\mathcal{M}$ determines the bit rate and robustness; higher-order modulations encode more bits per symbol but are more susceptible to noise.

2.1.2 Time-Domain Transformation (IFFT)

The frequency-domain symbols X_k are converted into a time-domain signal $x[n]$ using the Inverse Discrete Fourier Transform (IDFT), which is defined

as:

$$x[n] = \text{IDFT}\{X_k\}[n] = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} X_k e^{j\frac{2\pi nk}{N}} \tag{2.1}$$

where $x[n]$ represents the n-th sample of the OFDM symbol in the time domain. In practice however, this is implemented efficiently using the Inverse Fast Fourier Transform (IFFT).

2.1.3 Demodulation (FFT)

At the receiver, assuming perfect synchronization and channel estimation, the received time-domain samples $y[n]$ are converted back to the frequency domain using the Discrete Fourier Transform (DFT), implemented via the FFT:

$$Y_k = \text{DFT}\{y[n]\}[k] = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} y[n] e^{-j\frac{2\pi nk}{N}} \tag{2.2}$$

The recovered symbols Y_k are then demodulated to retrieve the original binary data. In the context of ranging, the preservation of the phase information in Y_k is critical for estimating the time of flight.

2.1.4 Cyclic Prefix (CP)

In OFDM, the Cyclic Prefix (CP) is usually used to prevent Inter-Symbol-Interference (ISI), while also to helping the performance of the FFT by transforming the linear convolution into a circular one. ISI is caused by multipath interference of symbols sent, meaning that the original signal and time shifted echoes are added together at the receiver. CP takes the tail of a symbol and prepends it to the current symbol, essentially nulling the interference as long as the CP length is at least the length of the longest echo.

2.2 Time of Arrival Estimation

Calculating the distance between devices relies on the precise estimation of the Time of Arrival (ToA) of the ranging signal. In Wi-Fi systems like IEEE 802.11az, this process exploits the Long Training Field (LTF), which acts as a known pilot sequence. The estimation process typically follows three main steps:

2.2.1 Channel Frequency Response (CFR) Estimation

The receiver transforms the received time-domain symbol $y[n]$ into the frequency domain Y_k using an FFT. Since the transmitted sequence X_k is known

(or locally generated in the case of Secure HE-LTF), the receiver can estimate the channel response on each subcarrier:

$$\hat{H}_k = \frac{Y_k}{X_k} = \frac{H_k X_k + W_k}{X_k} = H_k + \frac{W_k}{X_k} \tag{2.3}$$

where H_k is the true channel response and W_k is the noise. This vector $\hat{\mathbf{H}}$ represents the channel's attenuation and phase shift at each frequency.

2.2.2 Channel Impulse Response (CIR)

To identify individual signal paths (multipath components), the receiver converts the CFR $\hat{\mathbf{H}}$ back to the time domain using an IFFT. This yields the Channel Impulse Response (CIR) $h[n]$. In the CIR, the different multipath components appear as peaks at different time indices corresponding to their propagation delays.

2.2.3 Time of Flight and First Path Detection

The Time of Flight (ToF) corresponds to the path traveled by the signal that arrives earliest, known as the "First Path" (which represents the Line-of-Sight path if one exists). The receiver analyzes the magnitude profile $|h[n]|$ to identify this first significant peak. Simple thresholding or more advanced algorithms (e.g., super-resolution techniques like MUSIC [1] or ESPRIT [2]) are used to estimate the precise fractional delay τ of this first path. The estimated ToA is this delay τ relative to the start of the reception window. This notion is further used in augmenting the single round-trip packet into multiple round trips in order to mitigate multipath effects and improve ranging accuracy.

2.3 Secure Ranging and IEEE 802.11az

The Fine Timing Measurement (FTM) protocol enables devices to estimate distance by measuring the Round Trip Time (RTT) of signals. IEEE 802.11az improves this with secure FTM (sFTM) to prevent distance manipulation. The core of this security enhancement lies in the Secure High Efficiency Long Training Field (Secure HE-LTF). Furthermore, the choice of coding (BCC or LDPC) and rate (e.g. 1/2) is left to constructors. For further information on this, refer to [3].

2.3.1 HE-LTF Physical Characteristics

IEEE 802.11az (Next Generation Positioning) leverages the High Efficiency (HE) physical layer defined in the IEEE 802.11ax (Wi-Fi 6) standard. Consequently, the Secure HE-LTF inherits its physical characteristics from the

802.11ax HE-LTF, which was designed for robust performance in outdoor multipath environments. Key physical layer characteristics include:

- **4x Symbol Duration:** Compared to legacy Wi-Fi (802.11a/g/n/ac) which uses a 3.2μs symbol duration with a 64-point FFT (for 20 MHz), the HE-LTF uses a 4x larger FFT size (256-point for 20 MHz) resulting in a symbol duration of 12.8μs. This longer duration improves robustness against inter-symbol interference in channels with long delay spreads.
- **Subcarrier Spacing:** The subcarrier spacing is reduced from 312.5 kHz to 78.125 kHz.
- **Guard Interval:** HE-LTF supports various Guard Intervals (GI), including 0.8μs, 1.6μs, and 3.2μs. This GI contains a CP, which by nature leaks information on the end of the symbol.

2.3.2 Security Enhancements

Unlike legacy LTFs which use static, well-known sequences, the Secure HE-LTF utilizes cryptographically generated pseudo-random sequences. These sequences are derived using an AES-128 counter mode generator, ensuring that the transmitted signal is unpredictable to any eavesdropper who does not possess the shared secret key. This unpredictability is crucial for preventing Early-Detect/Late-Commit (ED/LC) attacks, as the attacker cannot predict future samples of the symbol to preemptively transmit them, unless they learn cryptographic secrets.

As previous iterations on securing ranging technologies required a short symbol, in OFDM-based ranging the symbols are long but do not suffer from the same issues as for instance Ultra-Wide-Band (UWB) ranging [4]. Furthermore, as modulation order increases entropy of the signal, it is recommended (although left as a choice to the constructor) to use 64QAM or even 256QAM [5].

Physical layer characteristics are also optimized for security:

- **No Cyclic Prefix (Zero Power Guard Intervals):** Secure HE-LTF symbols do not use a Cyclic Prefix as it would leak information about the symbol's content before it is fully transmitted, giving an advantage to an early-detect attacker. Instead, 802.11az keeps the spacing between symbols by using Guard Intervals which have zero power. This allows the system to be resilient against Inter-Symbol-Interference while giving no prior information on the random sounding sequence
- **No Pilots:** Pilot tones, which are typically inserted for channel estimation and phase tracking, are removed in the Secure HE-LTF to eliminate deterministic structures that an attacker could exploit.

- **Multiple round-trips:** The Secure HE-LTF symbols can be sent over multiple round-trips. This reduces the probability of guessing a correct sequence for the attacker. Effectively, if the attacker had probability p of guessing the first sequence, then for n sequences the probability is p^n, which is lower (assuming a secure cryptosystem).

At the receiver, the integrity of the ranging measurement is verified by correlating the received signal with the locally generated copy of the expected secure sequence. A successful ED/LC attack would theoretically require the attacker to guess the sequence, which is statistically improbable. Practical attacks that attempt to amplify or replay the signal indiscriminately typically result in a degradation of the correlation peak quality or a significant drop in the Signal-to-Interference-plus-Noise Ratio (SINR), which can be detected by the receiver. Furthermore, The receiver can compute statistics (average, standard deviation, etc.) on the timing of the multiple packets, thus further improving the discrimination between a legitimate user and an "distance bounding" attacker.

2.4 Early-Detect/Late-Commit (ED/LC) Attacks

While reading this section, it is recommended to periodically look at the schematic 2.1 to get the space-time context of the attack, and for more information read [6]. For our purposes, ED/LC lies in the realm of Time-of-Flight (ToF) measurements . In fact, when an initiator tries to compute the distance to its responder, their distance is going to be linearly dependent on the RTT of a ranging signal. Consider that the initiator is at a distance d from the responder, approximating the fact that radio waves travel at the speed of light c, we have the following relation $\tau = d/c$. Hence, we can compute the distance just from the time τ the signal took to travel the distance d. Furthermore, we have to keep in mind that this is just a one-way distance, in reality we have to consider that the initiator has to receive a signal back to compute the time, thus doubling the τ. But because there is some processing involved, the responder takes time t_p to begin sending a signal back (this is not the case with sonar, ultrasound, or laser distance measurements, as you are only expecting the signal to bounce back off a surface). Putting it all together, we have that the distance is

$$d = \frac{c(t_r - t_s - t_p)}{2} \tag{2.4}$$

where t_s is the time at which the initiator sent the first signal, t_r is the time at which the initiator received a signal back, and t_p is the processing time of the responder. Now in ED/LC an attacker tries to recognize the signal as soon as it can (Early-Detect) using the information at their disposal, and sends the remainder of the signal (Late-Commit) at a higher gain than the legitimate

sender. Because of the capture effect, the attacker effectively overshadows the legitimate signal. Thus, making the receiver decode the attacker's signal, as the legitimate signal is considered to be noise because of its lower amplitude.

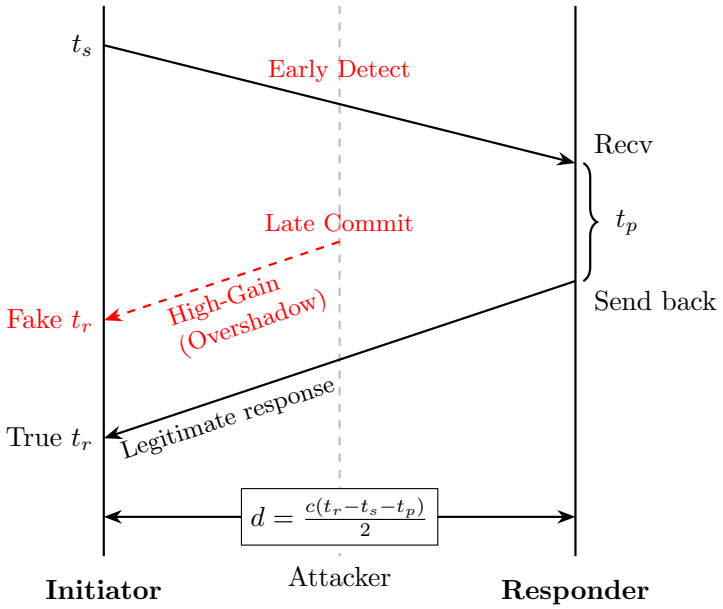

Figure 2.1: ED/LC attack single round-trip in a Message Sequence Chart format

Chapter 3

System and Threat Model

3.1 System Model

In general, we can assume that the adversary is has complete control over the wireless channel and can use any information at their disposal. In particular, we assume that the attacker is under the Dolev-Yao model. Secure FTM introduces an encryption mechanism, the secrets are supposed unknown to the attacker. This means that an sFTM signal looks like random symbols one after the other. The distance d is estimated based on the time of flight $\tau = d/c$.

3.2 Threat Model

We assume an external adversary $\mathcal{A}$ located at a position that allows interception and injection of signals. Furthermore, the attacker is assumed to have infinite sensitivity and can transmit at an arbitrary gain.

3.2.1 Adversary Capabilities

- **Oversampling:** The adversary may oversample the signal to gain a time advantage.
- **Early Detection:** The adversary attempts to infer the symbol S given only a fraction $p \cdot T_{sym}$ of the symbol duration.
- **Signal Injection:** Upon successful early detection, the adversary injects a late-commit signal to manipulate the timestamp.

Chapter 4

Implementation

This chapter describes the simulation framework developed to evaluate ED/LC attacks and the implementation of various attacker strategies.

4.1 Simulation Environment

The simulations are primarily conducted in Matlab, modeling the full OFDM TX/RX chain including channel effects. As previously mentioned, in our simulations we don't take into account the multiple roud-trips required for channel estimation and for reducing the probability of success of the attack (p^n instead of p, go back to section 2 on secure HE-LTF). Across the simulations, we vary the modulation order and number of OFDM subcarriers. The channel is implemented as AWGN and multipath is not taken into account as it would depend on many factors such as space geometry, and would further reduce the attacker's success rate, which we would like to avoid for a baseline.

4.2 Attacker Implementation

Here, we discuss the different attacker strategies, their implementation, prior theoretical background and hypothesis on their success. The early-detection strategies we have focused on are: Per-Tone-Slicing, Brute-Force and Viterbi Equalization. The first two represent the baseline and theoretical optimum respectively, and the latter is a widely used algorithm for general decoding. Lastly, we discuss the use of machine learning as an exploratory assessment of feasibility. The reader can refer to chapter 5 for the evaluation of such strategies and further explanations on the impact of modulation order and subcarrier count on attack effectiveness.

4.2.1 Per-Tone Slicing

The Per-Tone Slicing strategy serves as a baseline computational attack against the Secure HE-LTF. It represents the most fundamental approach where the attacker attempts to recover the transmitted sequence by analyzing the partially received OFDM symbol on a tone-by-tone basis, ignoring the effects of Inter-Carrier Interference (ICI) caused by the partial observation. It is important to note that we assume that the channel is a basic AWGN. This allows us to say that maximum-likelihood estimate is the same as computing the minimum Euclidean distance between the partially received symbol and expected symbols. Note that this would become even harder if, as the attacker, we had to guess the modulation for each symbol.

The attack procedure, as detailed in IEEE 802.11az documents [5], consists of the following steps:

1. **Partial Observation**: The attacker receives the first M samples of the time-domain OFDM symbol, corresponding to the observation period T_{ob} available before the Counter-Response phase begins.
2. **Zero-Padding**: To reconstruct a full-length OFDM symbol suitable for demodulation, the attacker appends $N - M$ zeros to the observed sequence, where N is the total number of samples in the OFDM symbol (FFT size).
3. **Frequency Domain Transformation**: A Fast Fourier Transform (FFT) is applied to the zero-padded signal to convert it back to the frequency domain.
4. **Slicing (Detection)**: For each subcarrier k, the attacker performs Maximum Likelihood (ML) detection. This involves calculating the Euclidean distance between the received complex value Y_k and all valid constellation points (e.g., QPSK, 16-QAM) defined by the Secure HE-LTF parameters. The point minimizing the distance is selected as the estimated symbol $\hat{S}_k$.

This method is computationally inexpensive but suffers from significant performance degradation due to the time-domain truncation (windowing). In signal processing terms, multiplying the time-domain signal by a rectangular window (the observation period) corresponds to convolving the frequency components with a sinc function. This spreads the energy of each subcarrier into its neighbors (spectral leakage), creating ICI. The Per-Tone Slicing approach treats each subcarrier independently, failing to compensate for this interference, which make it a lower-bound baseline for attack performance.

4.2.2 Brute Force Attack

This attack is as impossible as it is optimal. It is based on the presentation [7] by the IEEE task group. The Brute Force attack or Global Maximum Likelihood (ML) estimator does not entirely fit our threat model, as it assumes infinite precompute and instant lookup time. Nevertheless, we find it useful to discuss it from a theoretical standpoint, although the strategy is impractical for real life scenarios. Unlike Per-Tone Slicing, which makes independent decisions for each subcarrier, the Brute Force approach estimates the entire symbol sequence $\mathbf{S} = [S_0, S_1, \ldots, S_{N-1}]$ simultaneously.

The problem can be formulated as finding the sequence $\hat{\mathbf{S}}$ that, when transformed to the time domain and truncated to the observation window, minimizes the Euclidean distance to the received signal $\mathbf{y}_{obs}$:

$$\hat{\mathbf{S}} = \arg\min_{\mathbf{S} \in \mathcal{M}^N} \|\mathbf{y}_{obs} - \mathbf{W} \cdot \text{IFFT}(\mathbf{S})\|^2 \tag{4.1}$$

where $\mathcal{M}$ is the modulation alphabet (e.g., QPSK) and $\mathbf{W}$ represents the time-domain windowing operation (multiplying by a $rect(.)$ with T_{obs} for width).

This method perfectly accounts for the Inter-Carrier Interference (ICI) because every hypothesis $\mathbf{S}$ generates the exact ICI pattern that would be observed. However, the computational complexity is $\mathcal{O}(|\mathcal{M}|^N)$. For a typical configuration with $N = 244$ subcarriers and QPSK modulation ($|\mathcal{M}| = 4$), the number of hypotheses is 4^{244}, which is computationally infeasible. Furthermore, if we wanted to implement this in a real-world scenario, billions of correllators are required, which incurs an astronomically inhibitive price.

The Viterbi algorithm (described next) exploits the frequency locality of ICI (i.e., subcarriers mainly interfere with their immediate neighbors), allowing for a more efficient search.

4.2.3 Viterbi-based Early Decoding

The Viterbi approach (or Maximum Likelihood Sequence Estimation, MLSE) is a bit more sophisticated than the per-tone slicing attack. Here, we try to overcome the limitations of the baseline approach by treating subcarriers as dependent (as opposed to independent in per-tone slicing). The Viterbi algorithm therefore takes into account the ICI introduced by the partial observation.

In signal processing terms, the attacker's partial observation in the time domain is equivalent to multiplying the infinite-length signal by a rectangular window representing the observation period T_{obs}. In the frequency domain, this multiplication translates to a convolution of the original subcarriers with the window's frequency response (a *sinc* function). This convolution causes

the energy of each subcarrier to spill over into adjacent tones, resulting in ICI.

Next, we explain how the Viterbi decoding works and how it uses the trellis.

Trellis Structure

To apply the Viterbi algorithm, we treat the sequence of subcarriers as a time-series signal affected by Inter-Symbol Interference (ISI), where the "time" index corresponds to the frequency bin k. The algorithm operates on a trellis diagram defined by:

- **Memory Assumption:** We assume that the spectral leakage from a subcarrier significantly affects only its L immediate neighbors (e.g., $L = 2$). This finite memory allows us to state that the observed value Y_k depends only on the current symbol S_k and the previous L symbols (also called "taps" in the usual terminology).
- **States:** A state in the trellis represents the history of symbols required to compute the interference. For a modulation order M (e.g., $M = 4$ for QPSK) and memory length L, the state at step k is defined as the tuple $\sigma_k = (S_{k-1}, S_{k-2}, \ldots, S_{k-L})$. There are M^L total possible states.
- **Transitions:** As the algorithm moves from subcarrier k to $k + 1$, it transitions from state σ_k to σ_{k+1} by choosing a new symbol S_k. This shifts the history: $(S_{k-1}, \ldots, S_{k-L}) \to (S_k, S_{k-1}, \ldots, S_{k-L+1})$.
- **Branch Metric:** For each transition, the algorithm calculates a branch metric (cost) by predicting the expected observation Y_k^{pred} based on the hypothesized symbol sequence (determined by the transition) and the known channel filter (window function). The cost is the squared Euclidean distance $|Y_k - Y_k^{pred}|^2$.

The Viterbi algorithm efficiently searches this trellis to find the path (sequence of states) with the minimum accumulated cost, which corresponds to the Maximum Likelihood sequence estimate under the finite memory constraint.

4.2.4 ML-Based Early Detection

We also explored a deep learning approach using Convolutional Neural Networks (CNNs) to directly infer the transmitted symbols from the partial time-domain observation. The model architecture consisted of multiple 1D convolutional layers followed by fully connected layers, trained to minimize the cross-entropy loss between the predicted and true symbols.

However, this approach yielded poor performance in our experiments, failing to surpass the baseline Per-Tone Slicing method. We hypothesize that the neural network struggled to learn the inverse of the spectral leakage function

(the sinc convolution) effectively from the limited training data, whereas the Viterbi algorithm explicitly models this physical phenomenon. Given these results and the high computational cost of training, the AI-based method was not pursued further.

Chapter 5

Evaluation

5.1 Experimental Setup

We compute the bit-error-rate (BER) for random sounding 122-datacarriers signal, for different OFDM configurations (BPSK, QPSK, 16QAM, 64QAM). This allows us to compute the cumulative distribution of the BER for given modulation parameters. The strategy for the attacker is to decode a partially received signal. Masking an OFDM signal so that it only contains its first k bits, which introduces carrier-interference (ICI), making it difficult to decode on a per-tone basis. Usually a receiver would use the Viterbi decoder which implements the ML rule with relatively low complexity, and is optimal (for reducing BER) in AWGN channels.

5.2 Impact of Modulation Order and Subcarrier Count

5.2.1 Brute Force Attack

Here we only discuss theoretical bounds, as the software implementation of the attack would be computationally prohibitive.

We can assess the impact of the modulation order (M) and dimension (N) on the attack's success probability using the intuition that increasing the density of the constellation will increase P_e the probability of error. For the Brute Force ED/LC attack, the adversary must compute all partial reception windows for all constellation points. Furthermore, for a small reception window, there might be many candidate symbols, so the attacker has to wait until one clearly stands out to commit to it. Next, we discuss how these factors decrease the success rate of the attack.

- **Impact of the Modulation Order (M):** As M increases (e.g., QPSK to 16-QAM), the constellation points become denser. Consequently, the minimum Euclidean distance d_{min} between valid sequences decreases,

making them harder to distinguish in noise. This leads to a higher error probability P_e and reduced attack success.

- **Impact of the Subcarrier Count (N):** The number of competing hypotheses scales as M^N. While increasing N increases the dimensionality of the signal space (potentially increasing distance between random pairs), the exponential growth in the number of "distractor" sequences typically outweighs this benefit at low-to-moderate SNRs, leading to a degradation in performance or requiring exponentially higher SNR to maintain the same success rate.

In summary, the complexities being exponential on N and polynomial on M, together makes this attack effectively infeasible in real life.

5.2.2 Per Tone Slicing

Here we discuss how modulation order and number of subcarriers influence the bit error rate when decoding a partially received signal.

- **Impact of the Modulation Order:**

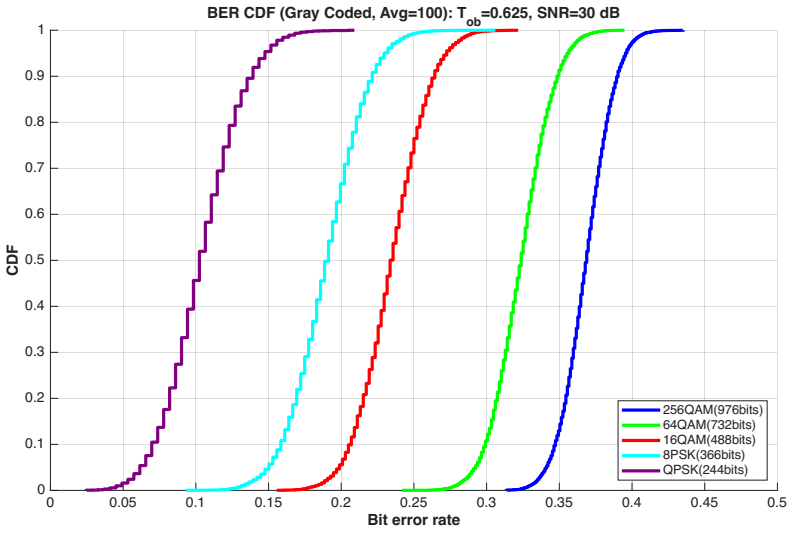

Figure 5.1: BER CDF for Per-Tone Slicing Attack (SNR=30dB, $T_{obs} = 0.625$).

As we can see on Figure 5.10 the bit error rate CDF, one can say that modulation order impacts the success probability of an attack. In fact, as you increase the order of modulation, the BER increases. This is expected, as the adversary has to guess constellation points from a larger probability space. As this plot is a reproduction of Figure 5.2 taken from [5], we can compare them one to one.

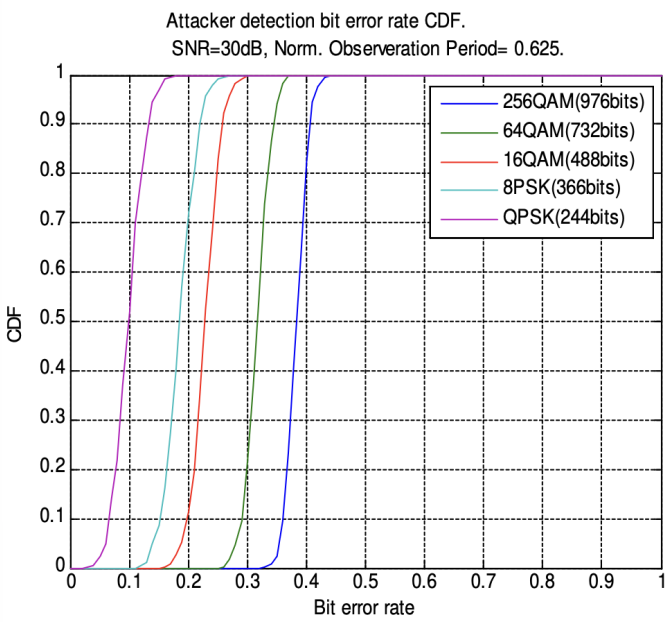

Figure 5.2: BER CDF for Per-Tone Slicing Attack (SNR=30dB, $T_{obs} = 0.625$).

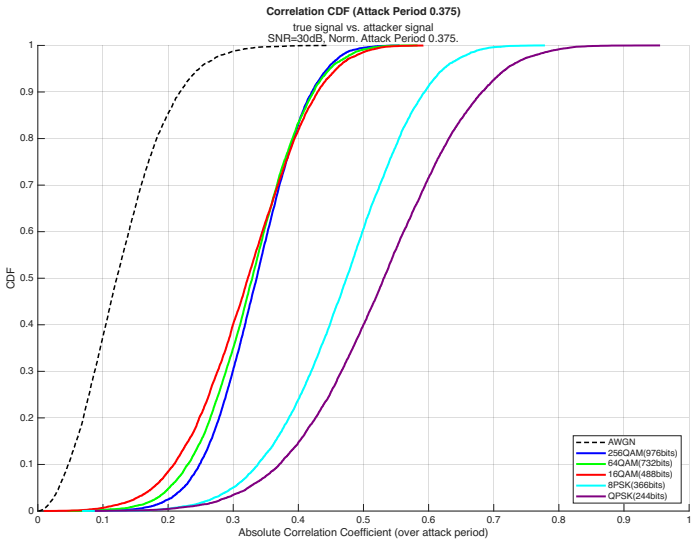

Figure 5.3: Correlation Coefficient CDF for Per-Tone Slicing Attack (SNR=30dB, $T_{atk} = 0.375$).

We could also look at the Correlation Coefficient (CC) of the signal sent by the attacker with the true signal. This is also done in [5] and comparing Figures 5.4 and 5.3 we see the same trend. Looking at the CDF of CC we notice that quadrature modulations bunch up together, as do the phase shifting ones.

From Figure 5.3 for each constellation, we note that, as expected, a

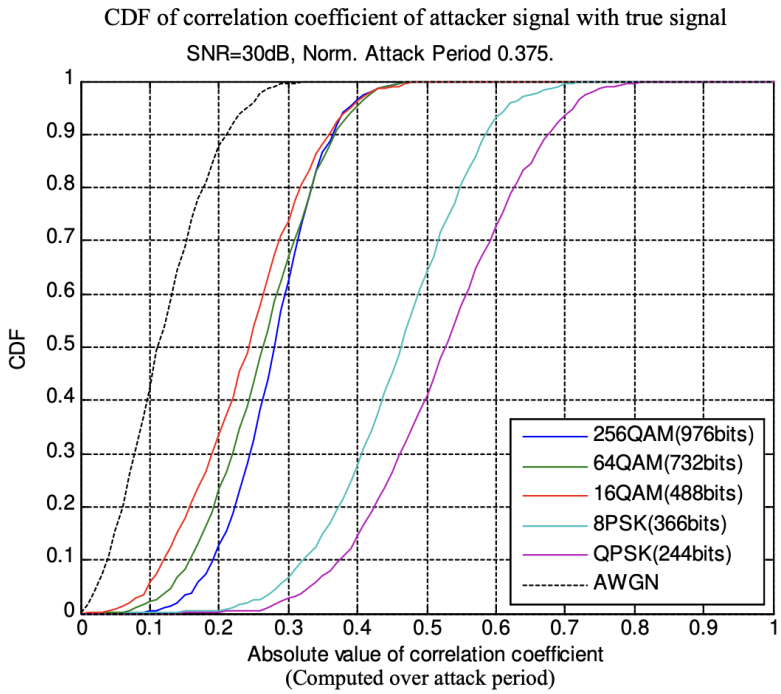

Figure 5.4: Correlation Coefficient CDF for Per-Tone Slicing Attack (SNR=30dB, $T_{atk} = 0.375$).

lower modulation order increases the chance of an attacker to generate a highly correlated signal.

- **Impact of the Subcarrier Count:** Increasing the subcarrier count, with a fixed bandwidth, reduces the inter-subcarrier spacing $\Delta f = \frac{B}{N}$, with B the bandwidth and N the number of subcarriers. But this directly impacts the observation time, and looking at a fixed observation ratio changes the picture.

  Our simulations (Figure 5.5) reveal that for a fixed observation ratio (e.g., observing 5/8 of the symbol), the mean BER remains largely constant between different FFT sizes. This is due to the scale-invariance of the Fourier transform: as N increases, the subcarriers become closer ($\Delta f \propto 1/N$), but the observation window T_{obs} increases proportionally, narrowing the spectral main lobes of the window function by the same factor.

  However, if we look at the same picture with an absolute (as opposed to a ratio of the symbol), we have the results in Figure 5.6. Here we can see that the FFT size impacts the BER inversely to the observation ratio. In fact, increasing the number of subcarriers while fixing the bandwidth is equivalent to decreasing the number of observed samples:

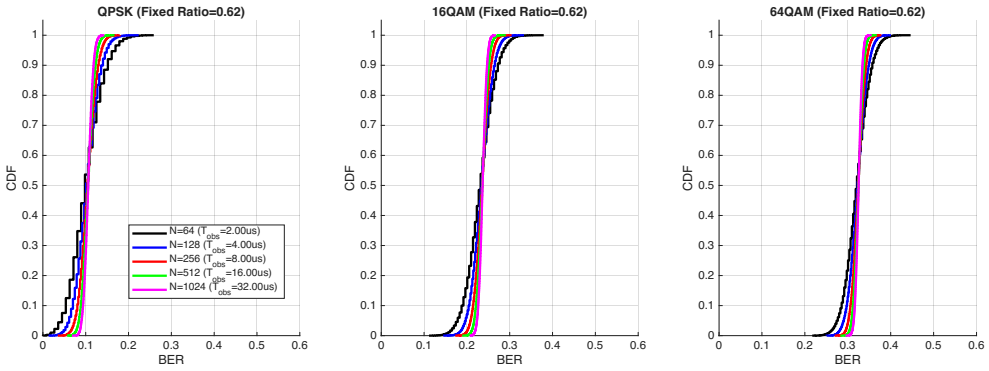

Figure 5.5: CDF of BER per FFT size (SNR=30dB, T_{obs}=0.625)

$$\Delta f = \frac{B}{N}$$

$$T_{symbol} = \frac{1}{\Delta f} = \frac{N}{B}$$

$$T_{obs} = T_{symbol} \cdot \text{Ratio} = \left(\frac{N}{B}\right) \cdot \text{Ratio}$$

$$n_{samples} = T_{obs} \cdot F_s = \left(\frac{N}{B} \cdot \text{Ratio}\right) \cdot (B \cdot o) = o \cdot N \cdot \text{Ratio}$$

where $F_s = B \cdot o$ is the sampling frequency and o the oversampling factor ($o = 1$ in critical sampling for complex signals and $o = 2$ for real valued signals) which can be set arbitrarily. Noticing this, we suppose that the observed decrease in variance in Figure 5.5 represents, in our simulations, a manifestation of the law of large numbers.

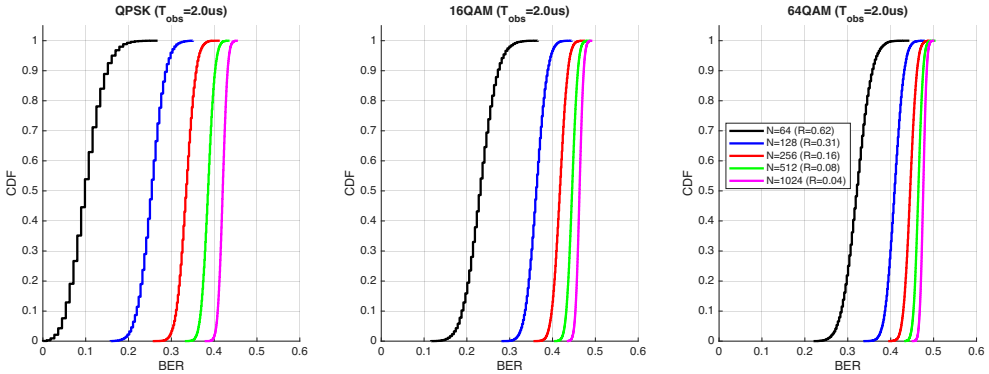

Figure 5.6: CDF of BER per FFT size (SNR=30dB, T_{obs}=2μs)

5.2.3 Viterbi Equalizer

We attempted to implement a Viterbi Equalizer to mitigate the effects of ICI and improve the attack success rate, as suggested by the IEEE 802.11az Task Group (TGaz).

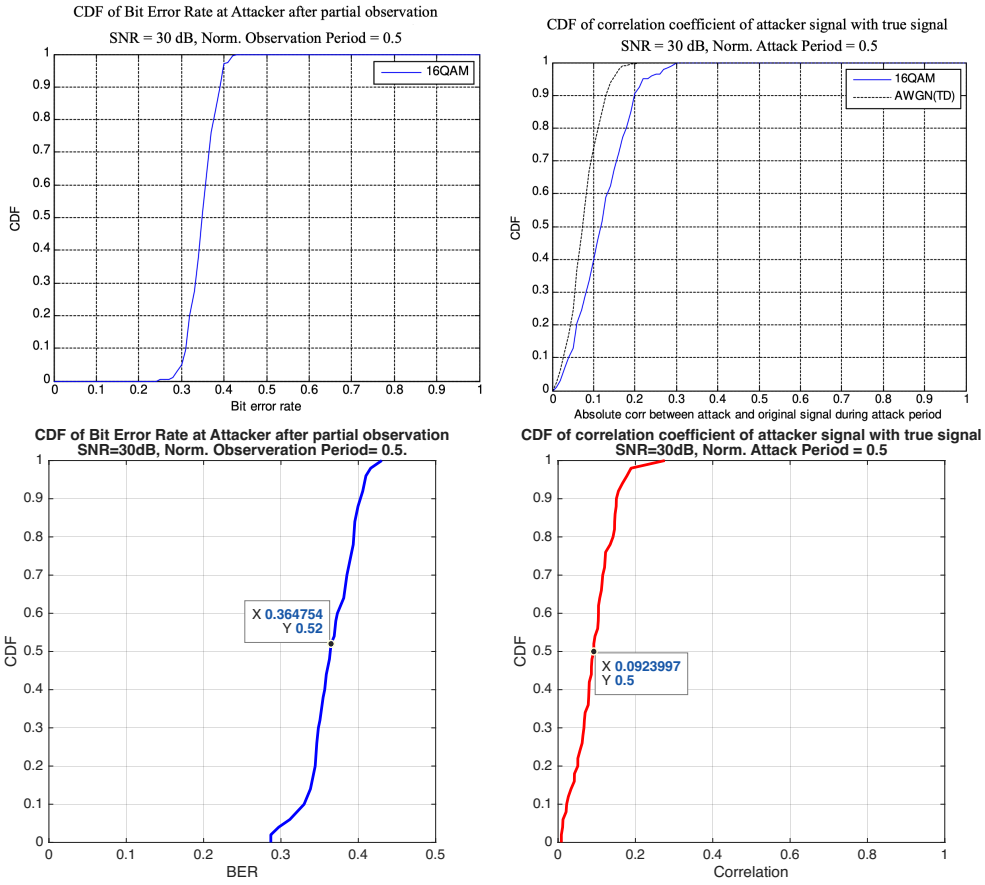

Figure 5.7: Comparison of BER CDF: TGaz Reference (left) vs. Our Implementation (right). Note the discrepancy in the slope and position of the curves.

Figures 5.7 illustrate the cumulative distribution function (CDF) of the Bit Error Rate (BER) and the CDF of the Absolute Correlation Coefficient (CC) of the signal during the attack period. The BER and CC seem to match the results of the TGaz in this case, for 16-QAM, an observation period of 1/2 and an SNR of $30dB$. However, our implementation yielded results that deviated significantly from the reference results for the other scenarios.

Similarly, the correlation results shown in Figure **??** do not align with the expected high correlation values presented in the TGaz documents (around 0.9 correlation). This further indicates a mismatch in the equalizer's parame-

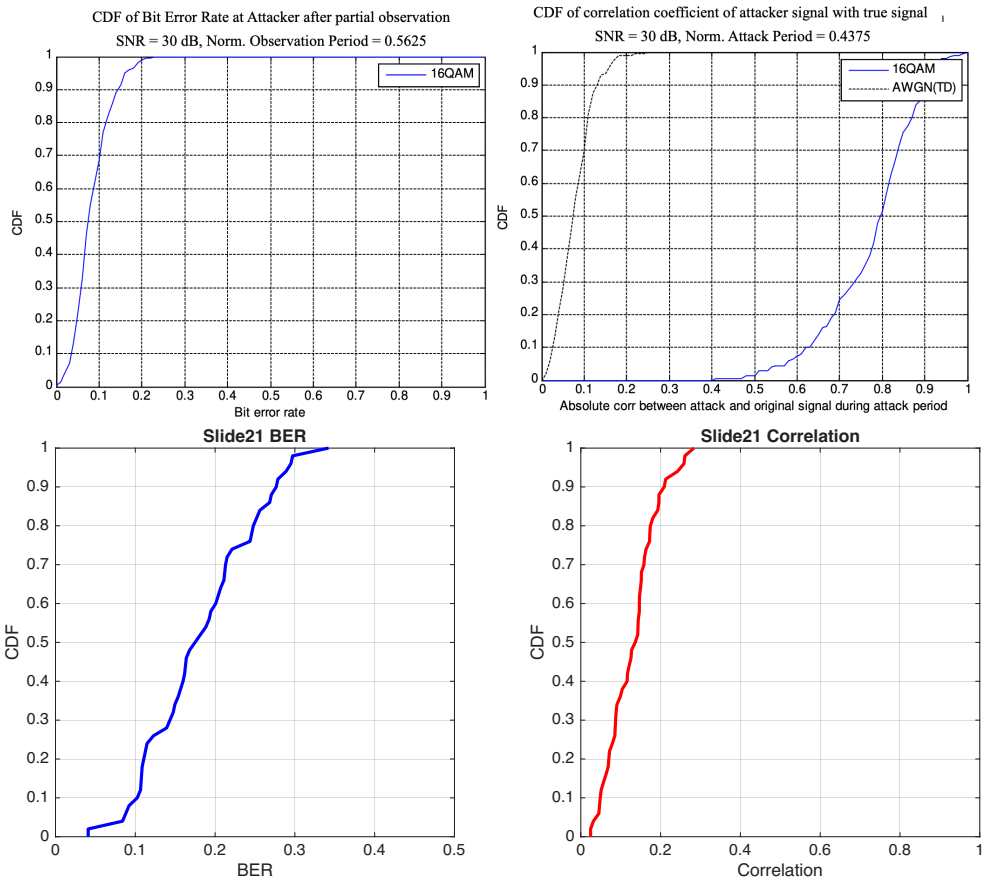

Figure 5.8: Comparison of Correlation CDF: TGaz Reference (left) vs. Our Implementation (right).

terization or state transition logic.

Further results comparisons can be found in the Appendix of this report for readability.

Despite these implementation challenges with the Viterbi equalizer, our results for the **per-tone slicing attack** (the baseline attack) are consistent with the IEEE baseline. We achieve very similar BER and correlation distributions for the per-tone slicing case, validating our underlying OFDM simulation and attack model. This suggests that the secure ranging parameters proposed by IEEE are indeed robust against standard per-tone slicing attacks, as confirmed by our reproduction of their baseline results.

5.2.4 ML approach

The ML based approach has yielded poor results, even compared to the baseline (Per-Tone Slicing). This indicates that the model is not able to

consistently invert the time-domain windowing to Inter-Carrier-Interference pattern. It could also stem from a bad implementation, either on the structure used for the CNN or in the hyper-parameters, although they were tuned with an optimizer (Optuna).

In Figure 5.9 we plotted the cumulative distribution function (CDF) of the bit-error-rate (BER) and of the Absolute Correlation Coefficient for the predicted remainder of the attack signal, for increasing modulation orders.

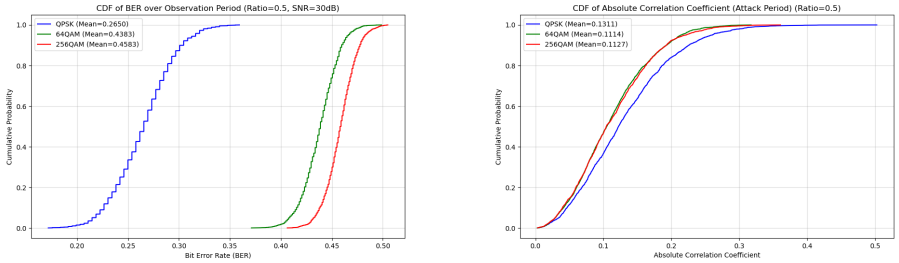

Figure 5.9: CDF of BER and CDF of Correlation coefficient for $T_{obs} = 1/2$

Here, for comparison we repeat the baseline results.

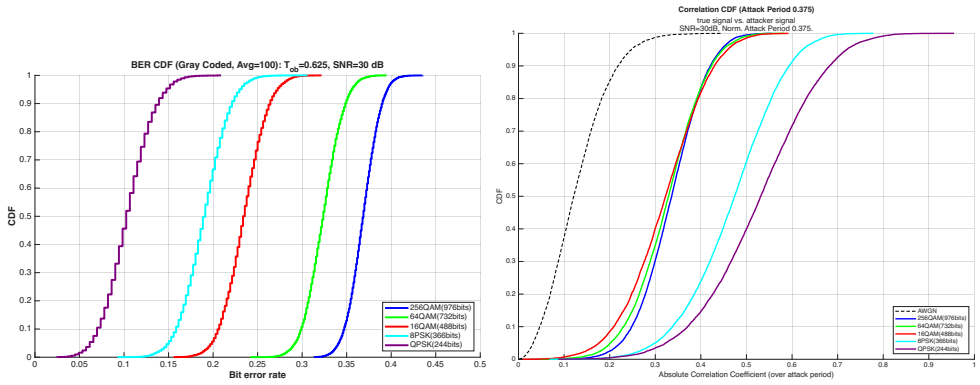

Figure 5.10: BER CDF for Per-Tone Slicing Attack (SNR=30dB, $T_{obs} = 0.625$).

Chapter 6

Conclusion

6.1 Summary

In this project, we analyzed the security of OFDM-based ranging against Early Detection / Late Commit (ED/CL) attacks. We focused on the per-tone slicing attack as a baseline and explored advanced strategies involving Viterbi equalization and Machine Learning predictions. Our simulations for the per-tone slicing attack closely matched the results reported by the IEEE 802.11az Task Group, confirming that the current secure ranging parameters provide a robust defense against this class of attacks. However, our attempt to reproduce the more sophisticated Viterbi equalizer attack revealed implementation complexities, leading to results that did not match the theoretical upper bounds shown in the standard's documentation.

6.2 Future Work

Several avenues for future research and improvement remain:

- **Fix Viterbi Equalizer Implementation:** The immediate next step is to revisit the Viterbi equalizer implementation. The discrepancy in our results (CDF of BER and Correlation) compared to the IEEE TGaz slides suggests errors in the ICI coefficient calculation or the trellis transition probabilities. Correcting this would allow for a proper evaluation of the Viterbi-based attack's success.
- **Turbo Equalizer:** Beyond the Viterbi algorithm, investigating Turbo Equalizers could provide better error correction performance. Turbo equalization iterates between separation and decoding, potentially recovering more information from the partial symbols than a single-pass Viterbi equalizer.

- **Custom ML/Approximation Approaches:** Finally, a more customized approach tailored specifically to the structure of the ED/CL attack on OFDM signals could be explored. This would likely require extensive knowledge of digital communications to derive likelihood functions or approximation methods that exploit the specific nature of the attack window.

Bibliography

[1] R. O. Schmidt, "Multiple Emitter Location and Signal Parameter Estimation," *IEEE Transactions on Antennas and Propagation*, vol. AP-34, no. 3, pp. 276–280, Mar. 1986. DOI: 10.1109/TAP.1986.1143830.

[2] A. Paulraj, R. Roy, and T. Kailath, "ESPRIT-Estimation of Signal Parameters via Rotational Invariance Techniques," *IEEE Transactions on Acoustics, Speech, and Signal Processing*, vol. 37, no. 7, pp. 969–985, Jul. 1989. DOI: 10.1109/ASSP.1989.32276.

[3] Y. Kim, "Ieee 802.11-18/1590r4," IEEE, Tech. Rep., September 2018. [Online]. Available: https://mentor.ieee.org/802.11/dcn/18/11-18-1590-04-00ax-d3-0-comment-resolution-part-1.docx.

[4] P. Leu, M. Kotuliak, M. Roeschlin, and S. Capkun, "Security of multicarrier time-of-flight ranging," in *Proceedings of the 37th Annual Computer Security Applications Conference*, ser. ACSAC '21, Virtual Event, USA: Association for Computing Machinery, 2021, pp. 887–899, ISBN: 9781450385794. DOI: 10.1145/3485832.3485898. [Online]. Available: https://doi.org/10.1145/3485832.3485898.

[5] T. Bin et al., "11az Secure LTF Design," IEEE, Tech. Rep., 2020. [Online]. Available: https://mentor.ieee.org/802.11/dcn/20/11-20-0836-00-00az-11az-secure-ltf-design.pptx.

[6] P. Leu, M. Kotuliak, M. Roeschlin, and S. Capkun, "Security of multicarrier time-of-flight ranging," in *Proceedings of the 37th Annual Computer Security Applications Conference*, ser. ACSAC '21, New York, NY, USA: Association for Computing Machinery, 2021, pp. 887–899. DOI: 10.1145/3485832.3485898.

[7] Q. Li et al., "On brute force attack to 11az secured mode," IEEE, Tech. Rep., 2020. [Online]. Available: https://mentor.ieee.org/802.11/dcn/20/11-20-0381-01-00az-on-brute-force-attack-to-11az-secured-mode.pptx.

Appendix A

Appendix

The code used in this work is available here: https://github.com/bybel/OFDM-ED-LC-Attacks

Here you can find the rest of the results comparisons between TGaz results and our own for the Viterbi Equalizer approach.

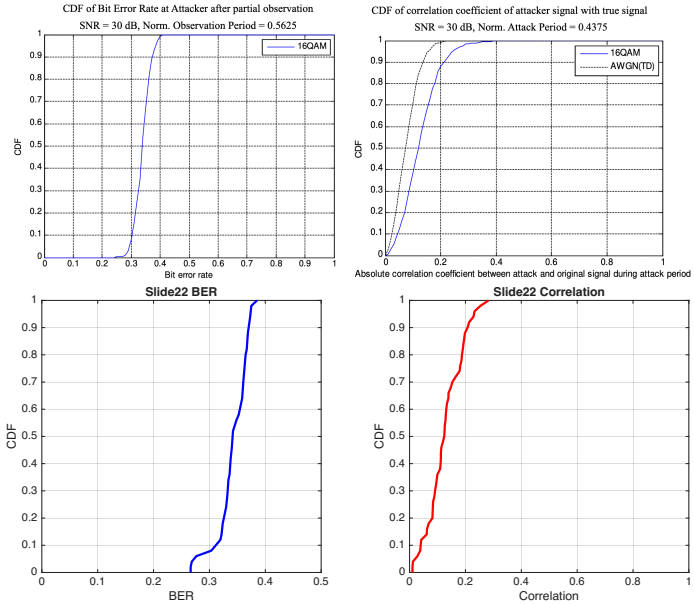

Figure A.1: Comparison of Correlation CDF: TGaz Reference (top) vs. Our Implementation (bottom).

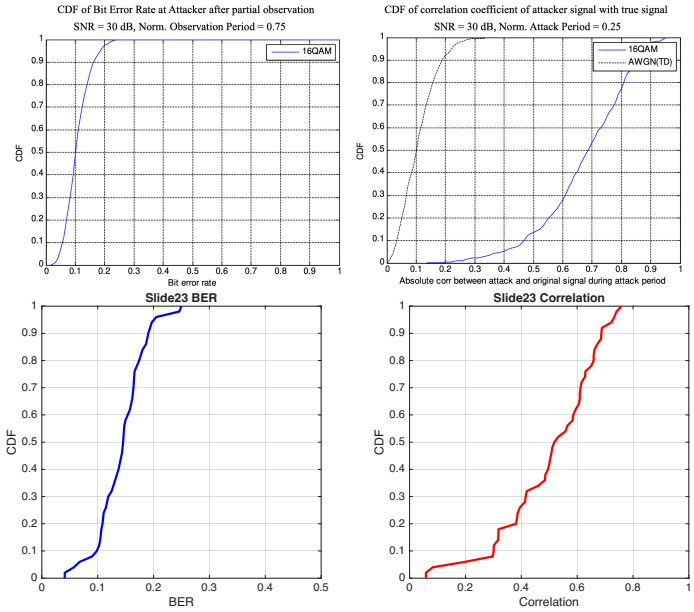

Figure A.2: Comparison of Correlation CDF: TGaz Reference (left) vs. Our Implementation (right).

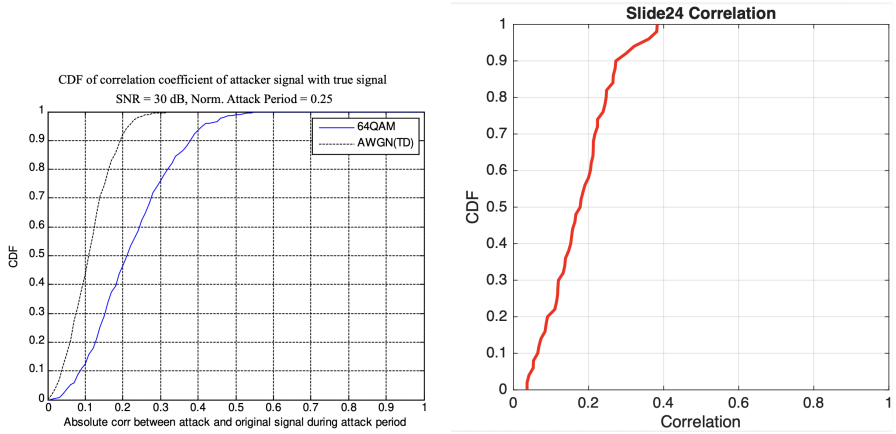

Figure A.3: Comparison of Correlation CDF: TGaz Reference (left) vs. Our Implementation (right).

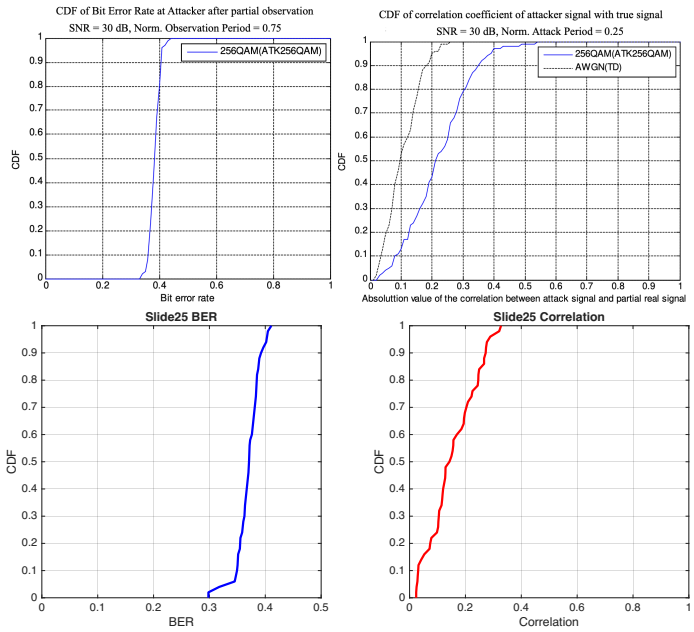

Figure A.4: Comparison of Correlation CDF: TGaz Reference (top) vs. Our Implementation (bottom).

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Declaration of originality

The signed declaration of originality is a component of every written paper or thesis authored during the course of studies. In consultation with the supervisor, one of the following three options must be selected:

○ I confirm that I authored the work in question independently and in my own words, i.e. that no one helped me to author it. Suggestions from the supervisor regarding language and content are excepted. I used no generative artificial intelligence technologies[1].

○ I confirm that I authored the work in question independently and in my own words, i.e. that no one helped me to author it. Suggestions from the supervisor regarding language and content are excepted. I used and cited generative artificial intelligence technologies[2].

◉ I confirm that I authored the work in question independently and in my own words, i.e. that no one helped me to author it. Suggestions from the supervisor regarding language and content are excepted. I used generative artificial intelligence technologies[3]. In consultation with the supervisor, I did not cite them.

Title of paper or thesis:

Analysis of OFDM-Based Rangingagainst Early-Detect/Late-Commit(ED/LC) Attacks

Authored by:
If the work was compiled in a group, the names of all authors are required.

Last name(s):	**First name(s):**
Flückiger	Raphaël

With my signature I confirm the following:

- I have adhered to the rules set out in the Citation Guide.
- I have documented all methods, data and processes truthfully and fully.
- I have mentioned all persons who were significant facilitators of the work.

I am aware that the work may be screened electronically for originality.

Place, date	**Signature(s)**
Zürich, 11/02/2026	Raphaël Flückiger

If the work was compiled in a group, the names of all authors are required. Through their signatures they vouch jointly for the entire content of the written work.

[1] E.g. ChatGPT, DALL E 2, Google Bard
[2] E.g. ChatGPT, DALL E 2, Google Bard
[3] E.g. ChatGPT, DALL E 2, Google Bard