

Executive Summary

Problem statement: Traditional Wi-Fi OFDM demodulation requires full-rate sampling for bit-level data extraction; unattainable under a power detector-based IoT device's sub-Nyquist sampling conditions.

Our Approach: We propose a Wi-Fi protocol compliant payload architecture that is decodable at the OFDM symbol level by comparing waveform similarities. Using low correlation reference OFDM symbols A and B, to encode binary data 0 and 1 respectively, we build an A/B symbol sequence to fill the payload, distinguishable even at downsampled conditions. The IoT device detects Wi-Fi packets through a preamble-based detection algorithm and decodes the payload using adjacent symbol-to-symbol correlation values.

Key contributions:

- Custom Genetic Algorithm for symbol design
- Power Detector-based Wi-Fi packet detection
- Robust adjacent symbol decoding algorithm

Background

Over 75 billion IoT devices are expected to be in use today due to their applicability in a wide range of industries and their low-power, light-weight computation; these benefits come at the cost of slow communication speeds.

Wi-Fi Backscatter: Prior research shows that backscatter communication using ambient Wi-Fi signals is a promising method to keep low-power benefits while increasing data transmission speeds. IoT tags piggyback data onto existing Wi-Fi signals by performing modulation algorithms that do not affect the traditional OFDM demodulation pipeline. Once modified, the tag reflects the signal to the intended RX. While uplink communication, IoT tag to RX, has been heavily researched, the downlink direction, TX to IoT tag, remains largely unexplored due to hardware constraints.

OFDM: IEEE 802.11a/g Wi-Fi uses OFDM with a 64-point FFT, distributing data bits across 52 active subcarriers at 20MHz bandwidth. The start of these packets contains a repeating symbol structure called the preamble which is used for detection and synchronization.

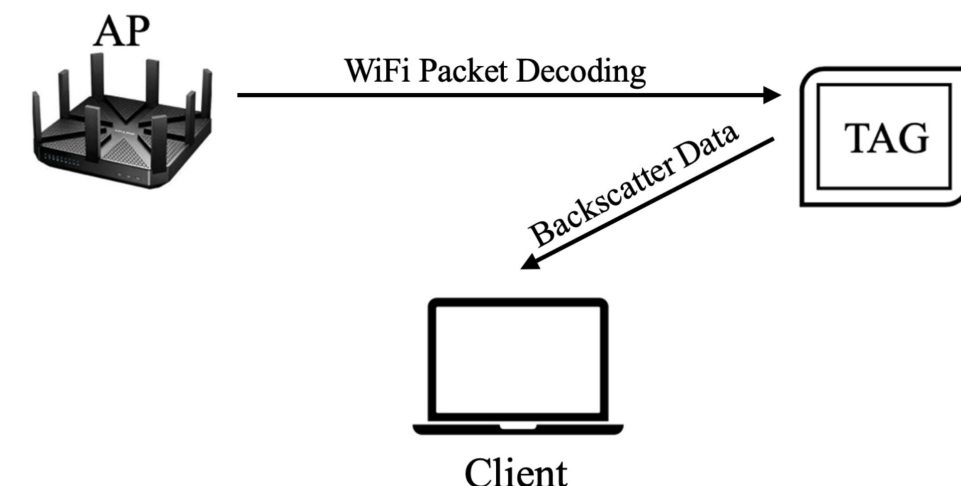


Figure 1. Wi-Fi Backscatter

Design Challenges

Absence of a Mixer: Captured Wi-Fi signals stay as passband signals instead of the usual baseband. When sampling with a power detector, the passband signal, which operates at high frequency, gets downsampled due to the limited bandwidth. This causes loss of information.

Phase Information Dropped: Signals are composed of phase (In-Phase) and amplitude (Quadrature) information. Power Detectors only capture amplitude (Voltage) data, losing phase information.

Pilot Subcarriers: Pilot subcarriers vary in OFDM symbols for the purpose of synchronization. Since our design is heavily dependent on waveform similarity, our design must take into account the pilot subcarriers effect on waveform.

CFO and CSI: Symbol distortion caused by a mismatch in internal frequency clocks and transmission through a channel.

Sampling Offset: Fine timing is necessary to find correct OFDM symbol boundaries to perform symbol-to-symbol cross correlation.

Packet Identification: Packet identification occurs in the upper layers of the Network Model. Since our IoT tag operates in the Physical Layer, the waveform must encode identification information.

System Design

Custom Packets: with the goal of staying Wi-Fi compliant, no changes were made to the packet structure. Payload bits were chosen based on intended symbol outcome modeled on the Wi-Fi transmitter side.

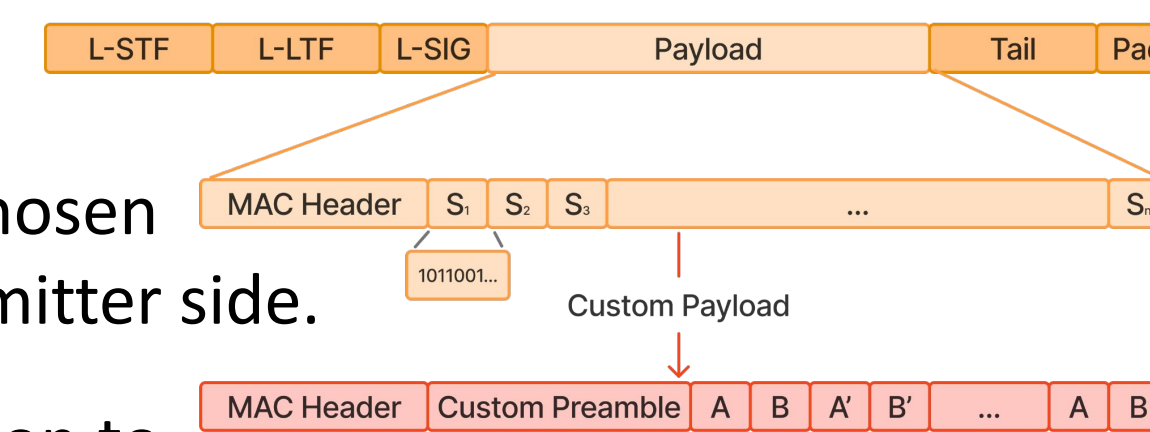


Figure 2. Packet Architecture

Packet Decoding: symbols are identified based on their correlation to the symbol preceding it. This algorithm mitigates the effects of CFO.

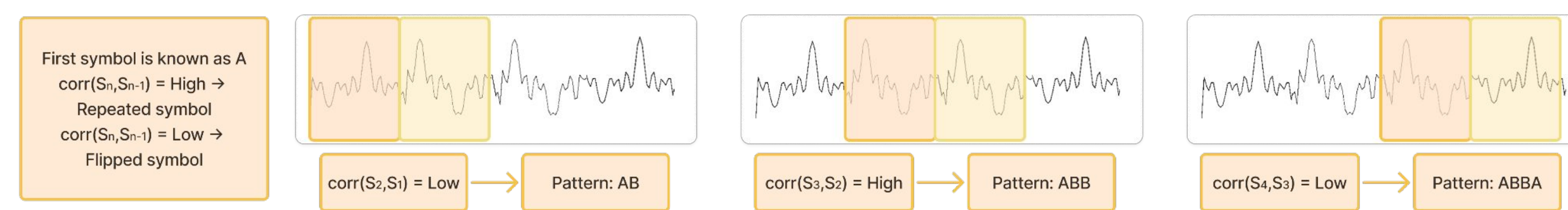


Figure 3. Correlation-Based Decoding Algorithm

WiFi Transmitter Side:

Genetic Algorithm - Because bits do not have a direct relationship with how the PD waveform will look, the bits are chosen based on “survival of the fittest” algorithm that starts with one symbol and goes through generations of mutation to find an opposite symbol that can survive real PD conditions.

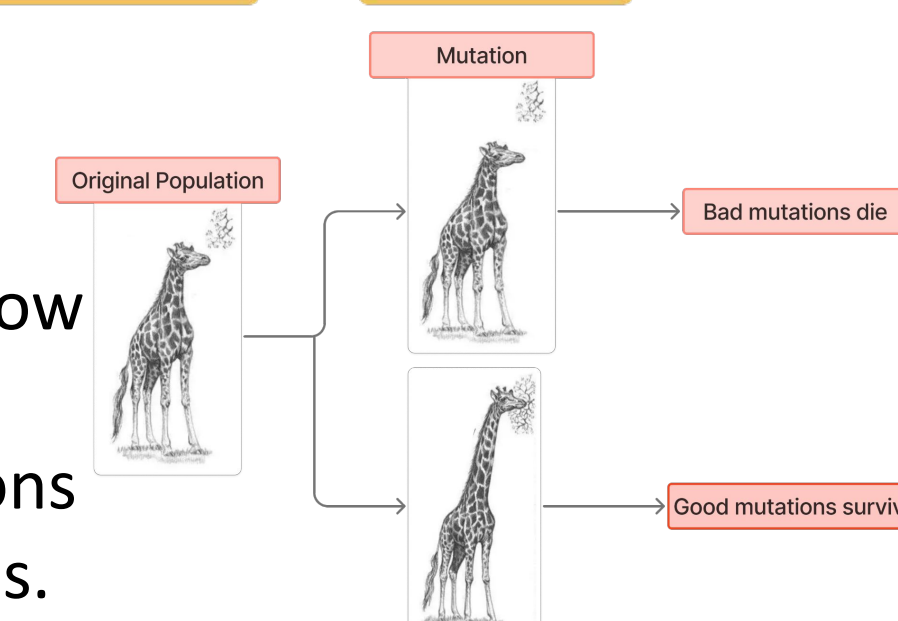


Figure 4. Survival of the Fittest

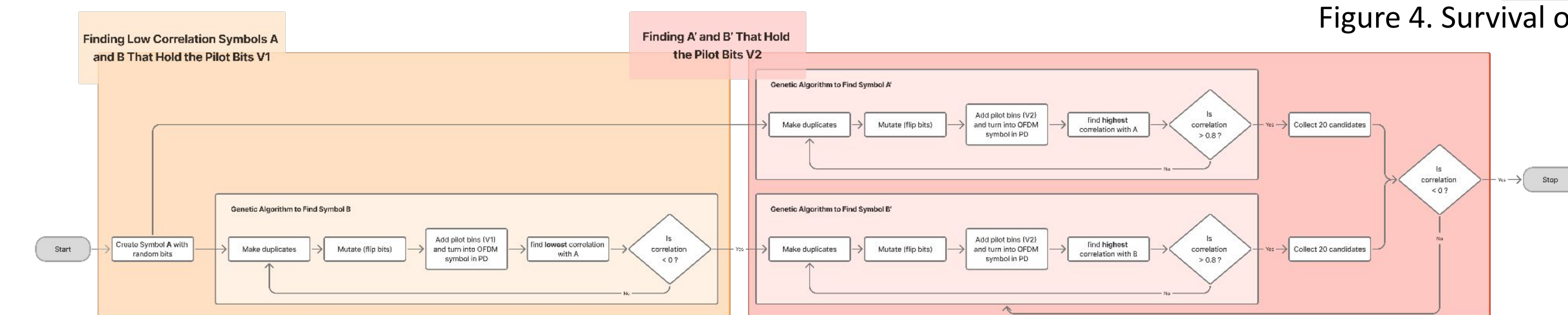


Figure 5. Genetic Algorithm Pipeline

IoT Tag Side:

Packet Detection - Different correlation sliding window sizes are used to detect the repeating symbol pattern of the preamble (L-STF & L-LTF) fields. If enough correlation values stay above a threshold for the entire length (8μs) of each preamble field, then a packet has been detected.

Payload Decoding - Symbol-to-Symbol correlation algorithm using a 40 sample sliding window.

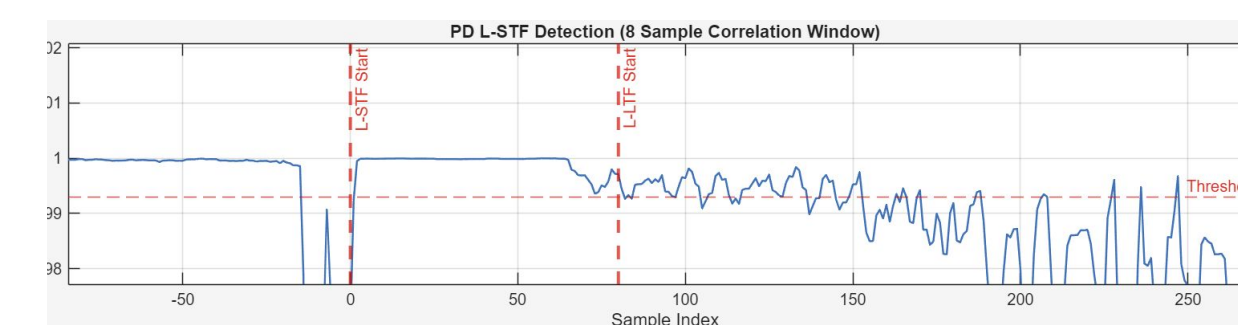


Figure 6. L-STF Detection

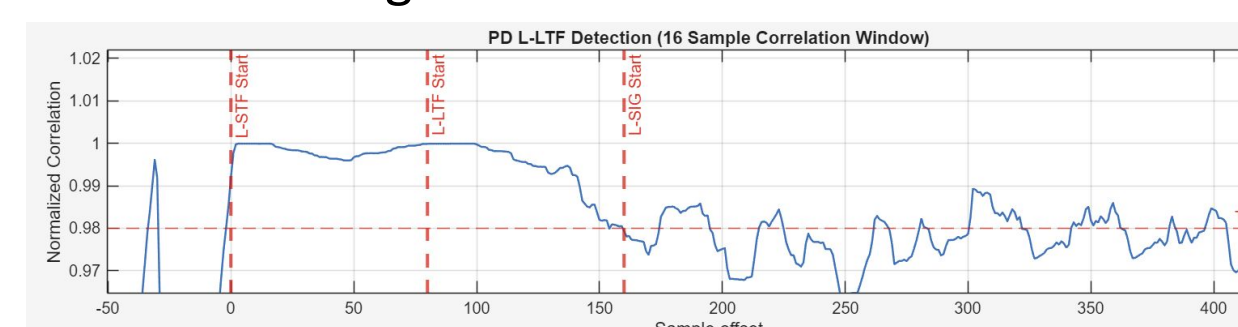


Figure 7. L-LTF Detection

Experimental Results

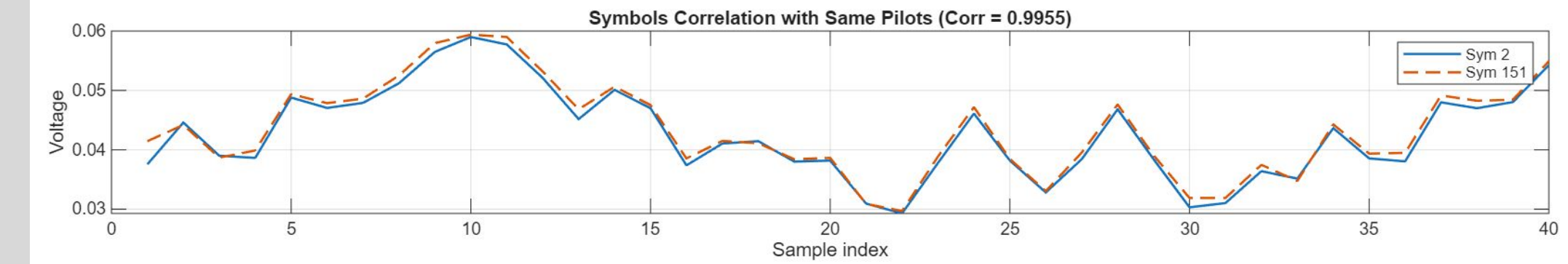


Figure 8. Effect of Same Pilot Subcarriers

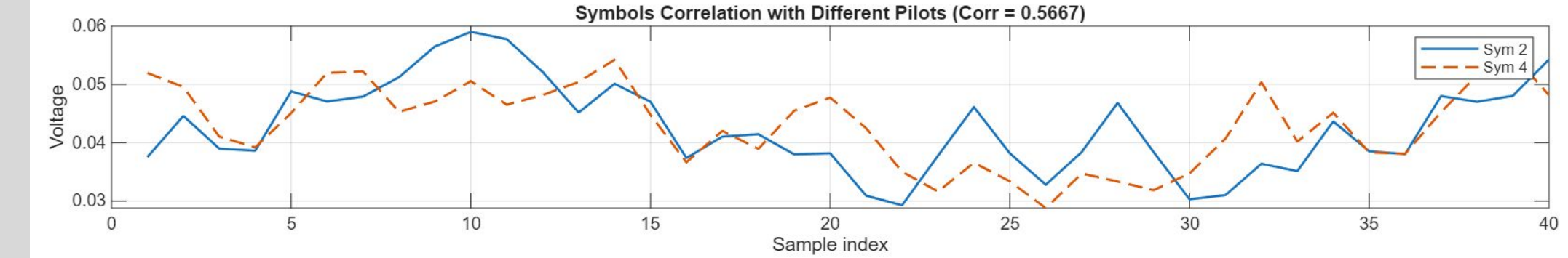


Figure 9. Effect of Different Pilot Subcarriers

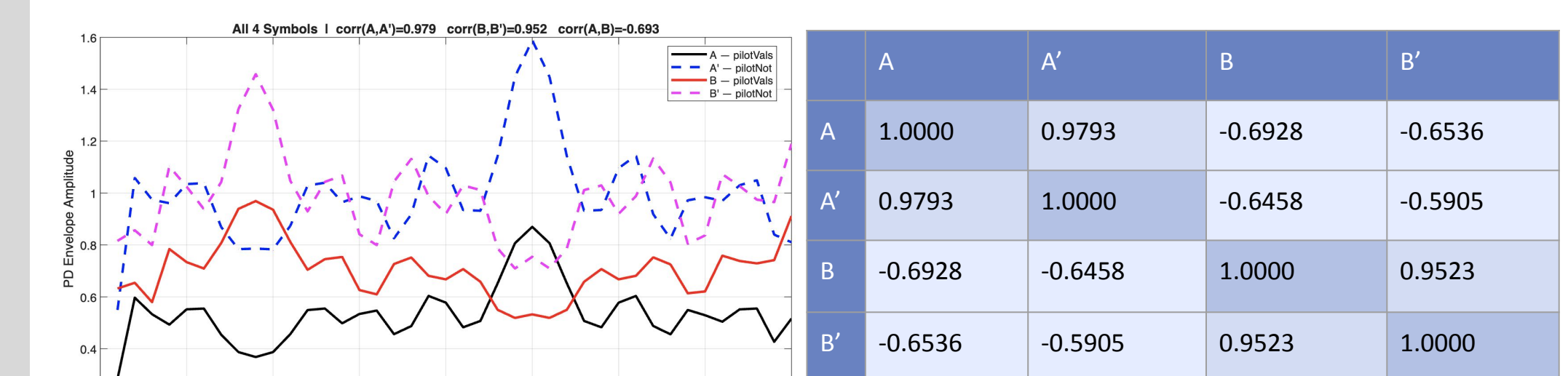


Figure 10. PD waveforms of Symbols produced by genetic algorithm

Table 1. Correlation of symbols produced by genetic algorithm

	A	A'	B	B'
A	1.0000	0.9793	-0.6928	-0.6536
A'	0.9793	1.0000	-0.6458	-0.5905
B	-0.6928	-0.6458	1.0000	0.9523
B'	-0.6536	-0.5905	0.9523	1.0000

Bits Found by Genetic Algorithm That Result in the Above Waveform

Symbol A bits: 100010000001101000001001101011011000001111110101
Symbol A' bits: 100010000101010101100101001101111110110110001
Symbol B bits: 010000100110000011010001101001001000011010011100
Symbol B' bits: 01000010010000010111000110000001000011000011000

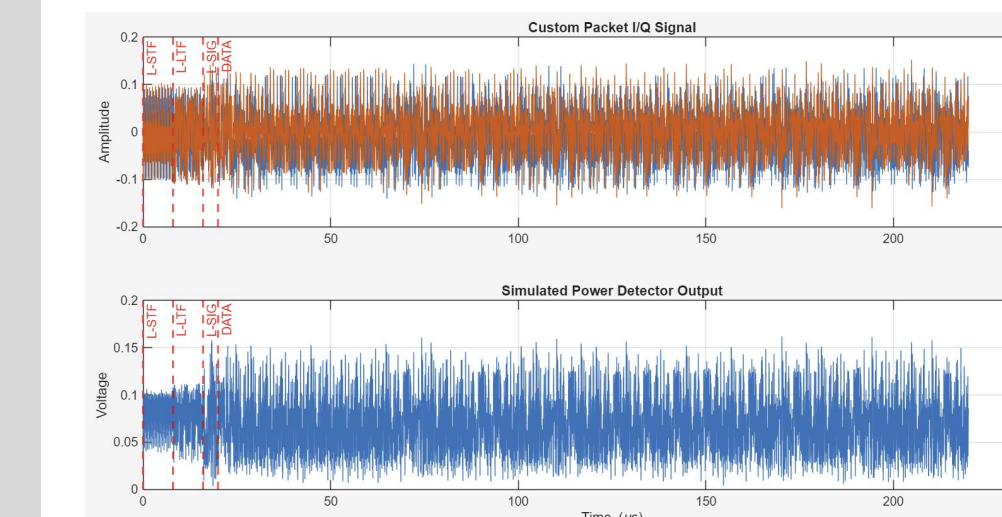


Figure 11. Received Signal

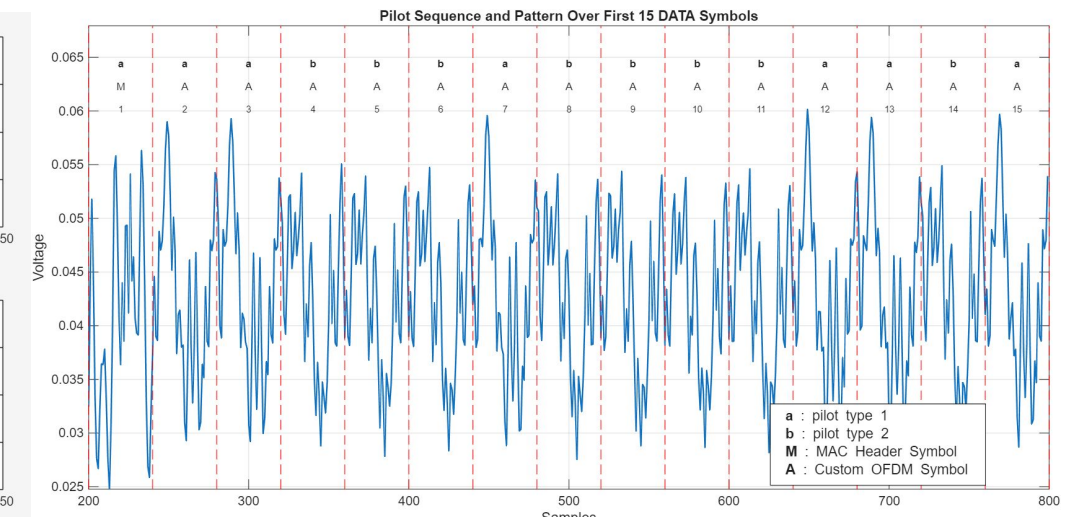


Figure 12. Zoomed in view of PD payload

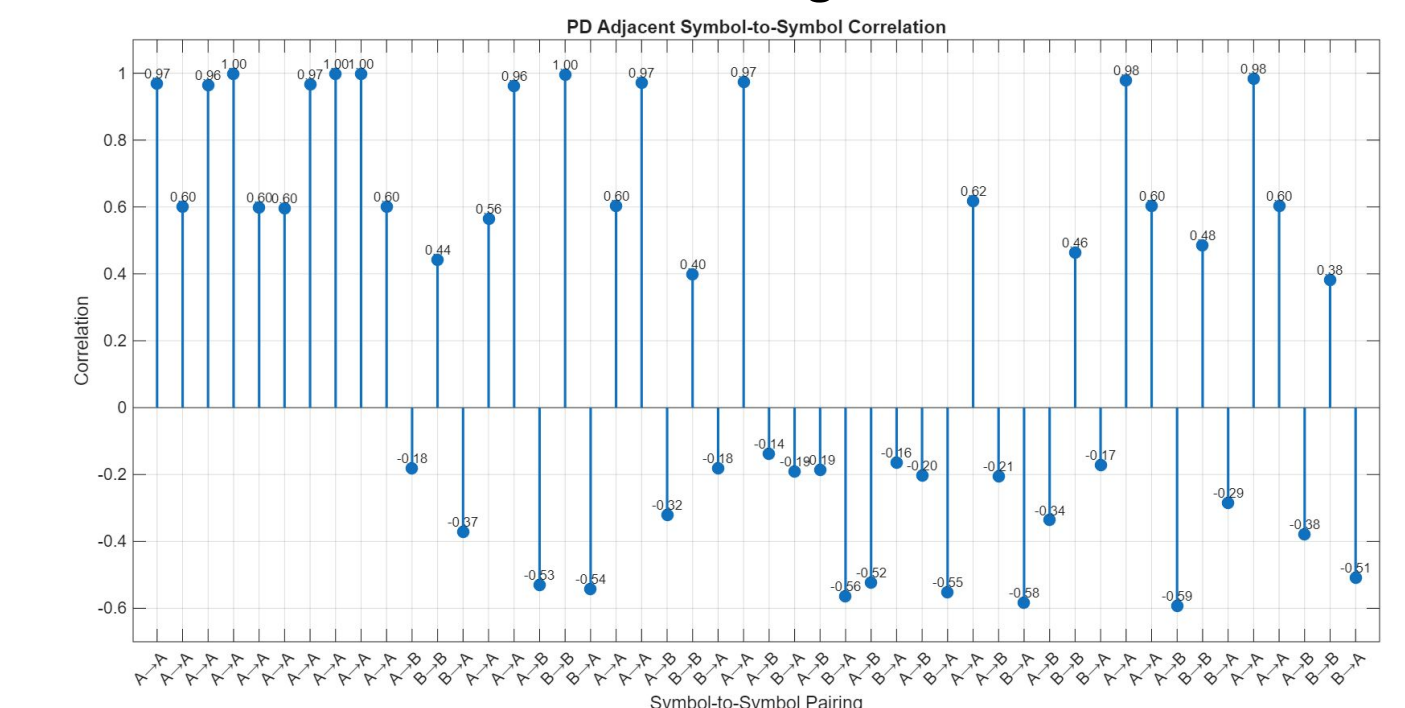


Figure 13. PD Symbol Correlation

Conclusions

Our preliminary experiments demonstrate strong and encouraging results; our low-correlation symbols A and B remain clearly distinguishable even at the power detector's downsampled rates, successfully proving the core concept of symbol-level payload decoding on low-power IoT devices. This enables reliable communication with low-power IoT devices using protocol-compliant Wi-Fi signals without requiring additional hardware. We will extend the testing to incorporate pilot-robust symbol pairs A' and B' using our multi-objective genetic algorithm. Moving forward, we plan to extend this work to support simultaneous communication between multiple IoT tags and to explore higher-order modulation schemes for improved performance. We sincerely thank Dr. Yoon Chae and Naeeb Ridwan for their valuable guidance throughout this project.

References

1. Yoon Chae, Zhenzhe Lin, Kang Min Bae, Song Min Kim, and Parth Pathak. mmcomb: high-speed mmwave commodity wifi backscatter. In Proceedings of the 21st USENIX Symposium on Networked Systems Design and Implementation, NSDI'24, USA, 2024. USENIX Association.