

Consumer-Friendly Spatial Anti-Jamming for WiFi Security Cameras

By
Alexander Bessonov
Everest Bencher
Michael Przybyl

Initial Report for ECE 445, Senior Design, Spring 2026 TA: Pusong Li
September 18th 2026 Project #33

Contents

1. Introduction	3
1.1 Problem	3
1.2 Solution	3
1.3 Visual Aid	4
1.4 High Level Requirements	4
2. Design	4
2.1 Block Diagram	5
2.2 Subsystem Overview and Requirements	5
2.2.1 Receive RF Chain Subsystem	5
2.2.1.1 Overview	5
2.2.1.2 Requirements	5
2.2.1.3 Components	6
2.2.2 Transmit Bypass Subsystem	6
2.2.2.1 Overview	6
2.2.2.2 Requirements	6
2.2.2.3 Components	6
Power Detect Subsystem	7
Overview	7
Requirements	7
Components	7
Control Subsystem	7
Overview	7
Requirements	8
Components	8
Power Subsystem	8
Constraints and Tolerance Analysis	9
Systems Budgeting	9
Criterion For Success	9
Limitations	9
Friendly Signals	9
Wide-Band Jammers	10
Sympathetic Nulls	10
Ethics, Safety and Societal Impact	10

1. Introduction

1.1 Problem

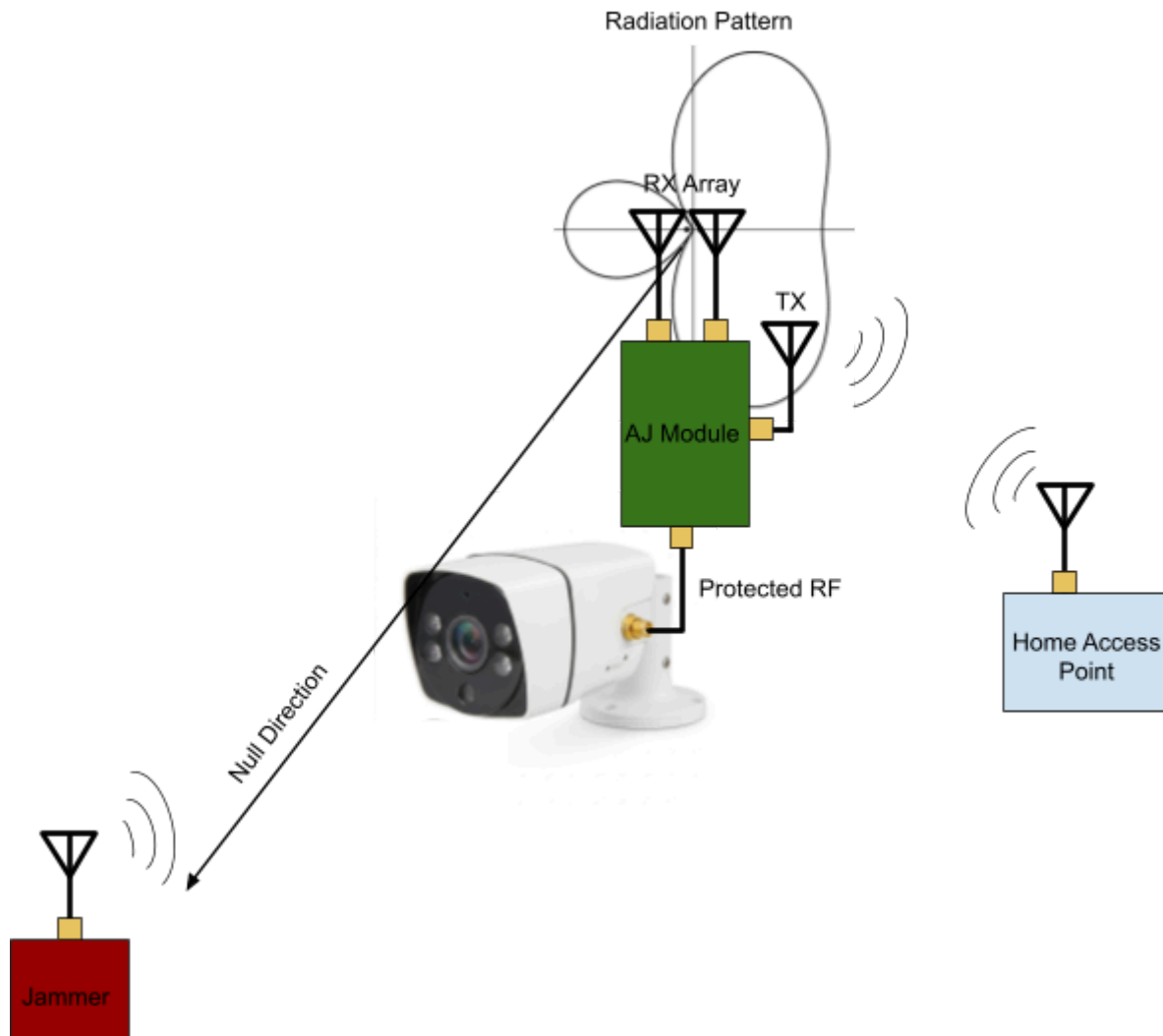
Today there are still numerous wireless systems still susceptible to malicious attacks from cheap RF jammers. Recent news articles report how burglars are using WiFi jammers to disable home security cameras before breaking and entering. These jammers are broad-band noise jammers that demand more than just digital filtering to mitigate, but spatial nulling at the antenna array. Conventional spatial anti-jamming (AJ) systems rely on high-speed digitizers and heavy signal processing to calculate adaptive weights. Having a digitization stage then forces the use of automatic-gain-control (AGC) to prevent ADC saturation. All said, this approach is impractical for size/cost/power constrained systems. Meanwhile, alternative countermeasures like spread-spectrum or frequency hopping technologies demand broad spectral allocations and have low bandwidth (non-ideal for video transmission). This motivates the development of a consumer-friendly solution for spatial AJ.

1.2 Solution

We propose a spatial AJ add-on module that would replace the rubber duck antenna on a typical 2.4 GHz WiFi security camera. The module features two SMA inputs for receive antennas, one SMA output for a dedicated transmit antenna, and one SMA port connecting directly to the camera's RF interface. The choice of a two element antenna array limits the scope of the project by reducing hardware and processing complexity.

The module would be able to null one adversary jammer and provide the end device with protected RF. Instead of digitizing the incoming RF, the module taps total signal power. The presence of a jammer would show up as a high power reading. An MCU monitors this power level and performs a gradient descent algorithm to tune the phase of one RF channel in order to minimize the jammer's effect. As a result, a deep spatial null is steered toward the jammer's direction.

1.3 Visual Aid

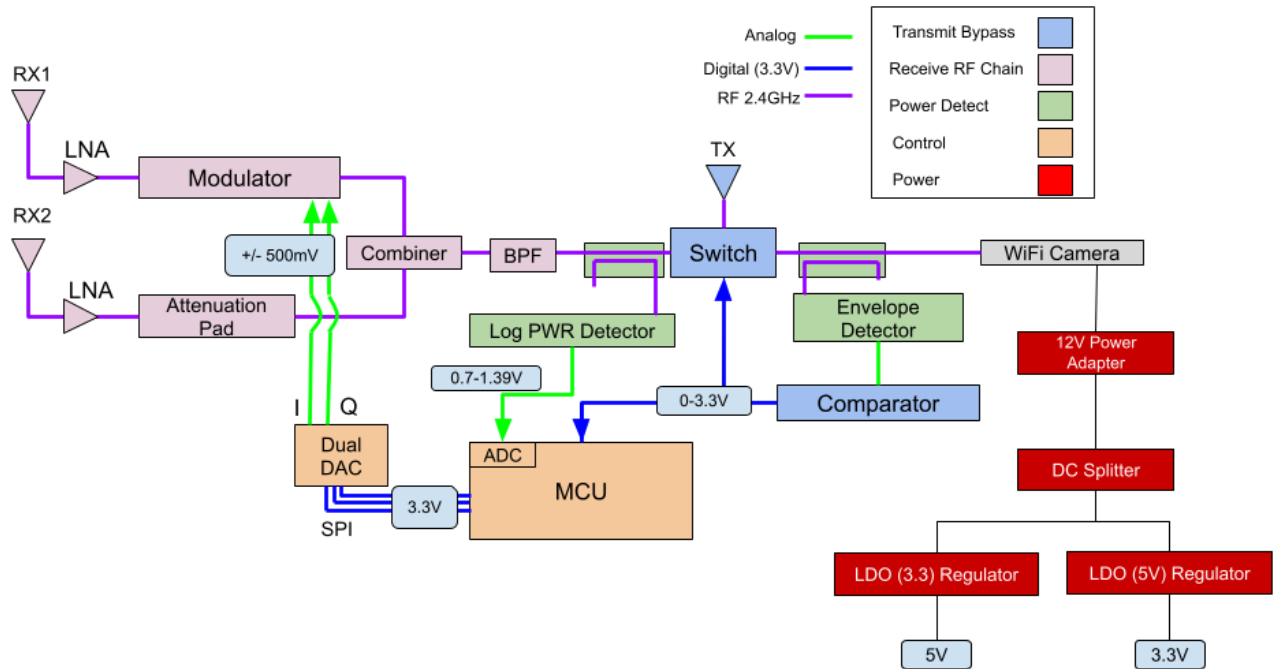


1.4 High Level Requirements

- At a high level, the module should mitigate an external jammer from overwhelming the camera's WiFi receiver by placing a spatial null of the radiation pattern in the direction of the jammer. The system must attenuate jammer power sufficiently to prevent saturation of the camera's LNA and maintain a minimum signal/jammer ratio required for continuous video streaming. The AJ module should offer a 20 dB null depth or better.
- The AJ module should not significantly degrade the friendly WiFi signal. Total system gain should be no lower than -3 dB and noise figure no greater than 15 dB. The AJ algorithm must not incidentally null the access point's WiFi signal.
- The module must be able to handle TX/RX switching to support bidirectional communication.

2. Design

2.1 Block Diagram



2.2 Subsystem Overview and Requirements

2.2.1 Receive RF Chain Subsystem

2.2.1.1 Overview

This subsystem serves as the front-end for the received WiFi and jammer signals. It begins with two SMA inputs for two antennas. Channel 1 routes through a RF vector modulator, which applies continuous phase adjustments based on control signals from the MCU. Channel 2 routes through a fixed attenuation pad to match the inherent insertion loss of the modulator, ensuring equal power levels between the channels. These two channels are summed into one through a RF combiner which produces the destructive interference in the direction of the jammer. The combined signal is then fed through a 2.4 GHz WiFi bandpass filter and passed to the power detect subsystem. This ensures that out-of-band signals or jammers don't unintentionally influence the AJ loop.

2.2.1.2 Requirements

This subsystem contributes to the high level requirements by performing the phase change and channel addition that causes destructive interference of the jammer.

- The inputs should interface with the antennas using SMA connectors. Both the inputs and outputs should present 50 ohm impedances
- The LNAs must have low noise figure and sufficient gain to compensate for the loss of the rest of the RF chain including in other subsystems
- Must be able to reliably apply phase change across all 360 degrees at WiFi frequency
- There must be sufficient filtering such that out-of-band signals don't influence the AJ loop during power detection

2.2.1.3 Components

- RF Modulator: AD8341
- Combiner: PD2425J5050S2HF
- Bandpass Filter: 2450BP15E0100001E

2.2.2 Transmit Bypass Subsystem

2.2.2.1 Overview

This subsystem detects high-power outgoing packets from the WiFi camera and immediately diverts these signals to the TX antenna. This is to ensure that outgoing signals are unimpeded and also protects the active circuitry in the receiver chain. It receives the rectified DC voltage envelope from the power-detect subsystem and feeds it into a high-speed analog comparator. The comparator compares against a voltage divider reference and triggers an RF switch that toggles between TX and RX modes. There is an alternative approach to this. If the target camera exposes an accessible PA enable logic line, it can directly toggle the RF switch and eliminate the need for the coupler+comparator stages. This may serve as an additional option.

2.2.2.2 Requirements

This subsystem contributes to the high level requirements by enabling the camera to send TX packets back to the access point and in turn allow bidirectional communication.

- The output should interface with the antenna using an SMA connector, and offer 50 ohm impedances to the input and output
- The time it takes for envelope detection, comparison, and switching must be sufficiently fast as to preserve the message's header packet and prevent damage to the receive front-end circuitry
- The RF switch must have sufficient isolation in order to prevent leakage from the TX antenna during receive mode and prevent leakage into the receive chain during transmit mode (>20 dB isolation)

2.2.2.3 Components

- Comparator: ADCMP600BKSZ

- RF Switch: SKY13453-385LF
- Envelope Detection Diode: BAT15-04W

2.2.3 Power Detect Subsystem

2.2.3.1 Overview

This subsystem taps RF energy from both transmission directions to supply feedback for both the spatial nulling algorithm and the transmit bypass logic. A forward -20 dB directional coupler taps a fraction of the combined receive signal and routes it to a logarithmic power detector, which converts RF power into a linear DC voltage for the MCU to read. A secondary -20 dB directional coupler taps reverse RF power originating from the camera during transmit bursts. This tapped reverse power is passed through a passive envelope detector, which produces a DC voltage response that the comparator in the TX bypass chain references.

2.2.3.2 Requirements

This subsystem contributes to the high level requirements by (1) providing the continuous power monitoring to the control subsystem in order to perform the nulling algorithm and (2) monitoring for TX packets so the transmit bypass subsystem can function accordingly.

- The RF inputs and outputs must present 50 ohm impedances. The power detector analog output must be within the MCU ADC's full-scale voltage. The envelope detector output must be within the comparator's input voltage range.
- The envelope detector must be able to detect TX bursts within 10 ns
- The power detector must function over a dynamic range from about -60 dBm to +5 dBm

2.2.3.3 Components

- Directional Coupler: CPJC-21-252R+
- Log Power Detector: AD8319ACPZ-R7

2.2.4 Control Subsystem

2.2.4.1 Overview

This subsystem executes the anti-jamming algorithm and drives the analog control voltages. An ESP32-S3 MCU samples the logarithmic power detector voltage and executes a gradient descent search. The algorithm tunes the IQ control voltages on the modulator which adjusts the phase of one channel and observes the power change to see if it was favorable in improving jammer nulling. Through multiple iterations, the null will eventually settle on the exact jammer direction. A dual DAC is needed for the MCU to produce the control voltages. To achieve better than 1 degree of resolution, a >8bit DAC is needed. The MCU's internal ADCs will be used to read the power detector output.

Added programming and thresholding would ensure the algorithm never tries to null the friendly WiFi signal. It will also ensure outgoing TX packets do not disturb the control loop. Finally, a toggle switch will act as the user interface to toggle AJ or pass-through modes.

2.2.4.2 Requirements

This subsystem contributes to the high level requirements by executing the nulling algorithm and producing the control voltages to the receive RF chain subsystem.

- The DAC must output IQ analog voltages that meet the requirements of the RF modulator through a differential converter
- The DAC must have sufficient bit resolution to allow better than 1 degree phase resolution

2.2.4.3 Components

- MCU: ESP32-S3
- Dual 10-Bit DAC: LTC1661CMS8

2.2.5 Power Subsystem

2.2.5.1 Overview

The power subsystem supplies the Wi-Fi camera and anti-jamming module from one regulated 12 V, 5 A external DC adapter. A two-way barrel-jack splitter distributes 12 V directly to the camera and to the anti-jamming board.

On the board, a buck converter reduces 12 V to an intermediate 5.5 V supply. A TPS7A2050PDBVR low-noise LDO generates the 5 V analog rail, while a TLV76733DRVR LDO generates the 3.3 V control rail. The 5 V rail powers the RF vector modulator and selected analog circuitry. The 3.3 V rail powers the ESP32-S3 and compatible control components.

Local bypass capacitors and bulk capacitance reduce supply disturbances. The PCB uses a continuous ground plane, with component placement and current-return paths arranged to limit coupling from the buck converter and MCU into sensitive RF and detector circuits.

2.2.5.2 Requirements

This subsystem contributes to the high level requirements by (1) supplying stable power to the vector modulator and MCU for jammer cancellation, (2) minimizing supply noise to preserve receive-chain performance, and (3) powering the comparator and RF switch for bidirectional communication.

- Distribute power from 12V, 5A adapter to the camera and the board.
- Provide a 5V rail up to 250mA for analog/RF circuitry.
- Provide 3.3V rail up to 600mA for the MCU and control circuitry.
- Reduce 12V to 5V and 3.3V using LDO regulators.

2.2.5.3 Components:

- LDO (5V):TPS7A2050PDBVR
- LDO (3.3V):TLV76733DRVR
- 12V, 5A DC Barrel Jack Adapter
- Two-way DC barrel power splitter

2.3 Constraints and Tolerance Analysis

2.3.1 Systems Budgeting

System performance is constrained by phase control resolution and channel gain imbalance. Calculations predict that with the phase resolution of a 10 bit DAC (0.35 degrees) and an arbitrary worst case 0.5 dB of channel gain difference, a theoretical null depth of 25 dB is possible. Accounting for real-world effects, we will target a 20 dB null depth which corresponds to a 99% reduction in jammer power.

System performance also depends on the WiFi camera receiver's J/S tolerance. Assuming the camera can operate at <10 dB J/S, and the module provides a 20 dB null depth, the max tolerable J/S at the module input is +30 dB. This can be used to compute the theoretical performance against a far-field jammer. If the WiFi signal is hitting the antenna at -50 dBm, this means the system protects against up to a -20 dBm jammer. This translates to a 1 W jammer positioned 10 feet away, which matches most real-world scenarios.

2.3.2 Criterion For Success

At a high level, the module should mitigate an external jammer from overwhelming the camera's WiFi receiver by placing a spatial null of the radiation pattern in the direction of the jammer. The system must attenuate jammer power sufficiently to prevent saturation of the camera's LNA and maintain a minimum signal/jammer ratio required for continuous video streaming.

In the event one or more subsystems fail to work either by design or due to logistics, a reduced scope plan will be put in place. The same construction would be made out of an eval board of the modulator (AD8341-EVALZ), a discrete combiner, and coax cables which feed into a spectrum analyzer. Benchtop voltage power supplies would control the modulator. An external PC running MATLAB will interface with the equipment via GPIB, reading power levels and executing the gradient descent loop to demonstrate jammer suppression on the spectrum analyzer display.

2.3.3 Limitations

2.3.3.1 Friendly Signals

Total power is direction and content agnostic. A nearby AP, a neighbor's overlapping-channel WiFi, Bluetooth, or even a burst of the camera's own uplink traffic could out-power the jammer momentarily

and get nulled instead. Evidently, configuring our anti-jammer to be just a blind power minimizer could easily null the camera's own AP if it's briefly the strongest thing in the room. We do intend on having additional programming and thresholding to identify and separate malicious signals, but it still runs a continuous risk of misidentifying good signals, thus destructively affecting our camera feed.

2.3.3.2 Wide-Band Jammers

Because the modulator applies a fixed phase shift to all frequencies rather than a true time delay, null depth degrades across the WiFi channel bandwidth meaning poorer performance toward the band edges. As a result, the AJ module would exhibit a reduced null depth against wide-band jammers.

2.3.3.3 Sympathetic Nulls

Sympathetic nulls are unintentional nulls created in the array pattern that can accidentally attenuate desired signals from the AP. To mitigate this risk, we suggest utilization of directional patch antennas. This configuration provides physical isolation against forward-facing jammers while significantly narrowing the angular sector where a sympathetic null could intersect the AP. However, spatial overlap risks remain depending on jammer geometry, necessitating further EM simulation to fully characterize these edge cases.

3. Ethics, Safety and Societal Impact

To ensure FCC compliance during testing, verification will take place on a cabled benchtop setup using RF signal generators. A signal generator will generate a CW jammer tone at the camera's WiFi channel frequency. This signal will pass through an RF splitter into two coax paths with calibrated phase (length) offsets. The WiFi signal is then embedded into each of these channels using standard 2.4 GHz antennas and combiners. Finally, each channel is fed into the module's inputs.

Initially, this composite signal will be injected into the camera without the AJ module in order to characterize the jammer/signal ratio where video streaming fails. Once established, the module will be installed. Success is demonstrating a ~20 dB improvement in jammer power tolerance while maintaining a continuous video stream. With measured null-depth, the theoretical over-the-air performance could be calculated with FSPL equations.

In terms of the societal impact, the problem statement for our project leans on increasing public-safety by making it more difficult for burglars to disable cameras before break-ins. Even though this is a valid motivation for developing our device, it raises an obligation under IEEE's honesty/realism canon and ACM's "comprehensive and thorough evaluation, including possible risks" principle: don't let the framing imply more protection than the device delivers.

Concretely, our prototype nulls **one** jammer, in a known/bounded geometry, up to a specific dynamic range, with a single spatial degree of freedom. A real attacker could use multiple jammers, move during the attack, or use power levels outside your tested range. If this project is ever pitched as a consumer safety product (even hypothetically in your report's future-work section), it's worth explicitly flagging that

a "jammer-resistant" claim could give homeowners false confidence and cause them to skip other precautions (monitored alarms, etc.), which could possibly even leave them in a less protected state.