Basic Concepts Understanding

Diagram/Tools

Detection and Mitigation of Unauthorized RF Signal Amplification in Keyless Vehicle Systems.

Items Needed for Statement of Work (SoW)

Prepared by

Muhammad Ali Nadeem

August 03, 2025

1. Introduction

The increasing integration of wireless technologies into modern vehicles has improved user convenience but simultaneously exposed vehicles to new forms of cyber-physical attacks.

One of the most prevalent security vulnerabilities involves relay attacks, wherein criminals exploit wireless key fob systems by amplifying or replaying legitimate radio frequency (RF) transmissions to gain unauthorized access to vehicles. These attacks exploit the inherent trust between the vehicle and key fob by relaying authentic signals rather than hacking the encryption protocols directly.

In recent years, Canadian law enforcement agencies have reported a significant rise in keyless vehicle thefts, many of which are linked to RF relay-based attacks. Traditional security mechanisms such as encryption and rolling codes fail to address this issue, as the problem lies not in decoding but in the unauthorized amplification or retransmission of legitimate signals.

My research aims to explore the physical-layer characteristics of RF transmissions—specifically around the 300 MHz frequency range commonly used by automotive key fobs—to develop a model capable of identifying, distinguishing, and blocking non-authentic, amplified, or tampered RF signals.

This study will integrate RF diagnostics, spectrum analysis, and firmware-controlled hardware design to deliver a practical detection and mitigation solution for keyless entry systems.

2. Problem

While existing keyless entry systems rely heavily on cryptographic security, they remain vulnerable to physical-layer exploits such as signal amplification and relay attacks. These attacks are particularly challenging to detect because they involve no modification of the transmitted data; instead, they *manipulate the signal strength, propagation delay, and temporal characteristics to deceive the vehicle into authenticating the transmission.*

The current gap in automotive cybersecurity lies in the absence of effective detection mechanisms at the RF signal level that can differentiate between a genuine nearby transmission and an amplified or relayed version.

Without such detection, vehicles cannot distinguish between legitimate proximity-based signals and those artificially extended beyond their intended range.

Problem statement: How can *authentic RF transmissions from automotive key fobs be effectively distinguished from amplified or tampered counterparts, and how can unauthorized signal amplification be detected and blocked in real time?*

3. Objectives

The primary objective of this study is to develop a detection and blocking model that can identify unauthorized signal amplification within the RF communication channel of keyless vehicle systems.

Specific objectives include:

1. Analyze and compare authentic RF transmissions with their amplified or tampered versions.
2. Develop a computational model that can identify non-authentic signals.
3. Design and prototype a circuit board integrated with firmware capable of monitoring and neutralizing unauthorized signals in real time.
4. Validate the model under experimental conditions using real automotive key fob signals.

4. Methodology

The research will adopt a multi-phase experimental methodology, combining theoretical modeling, RF experimentation, and embedded hardware design.

Phase 1: Data Acquisition and Signal Profiling – Collect authentic and tampered signals using RF analysis tools.

Phase 2: Feature Extraction – Identify distinguishing features using signal processing and machine learning.

Phase 3: Detection and Blocking Model – Develop algorithms to detect anomalies and firmware to neutralize unauthorized signals.

Phase 4: Hardware Implementation – Design a prototype integrating RF sensors and microcontrollers.

Phase 5: Evaluation – Assess performance using detection rate, false positives, and efficiency.

5. Expected Contributions

This study aims to make the following contributions:

1. Novel Detection Framework for unauthorized RF amplification.

2. Working Prototype capable of real-time detection and blocking.

3. Enhanced Automotive Security Standards.

4. Academic Contributions to RF forensics and physical-layer security.

6. Conclusion

This research addresses a critical and underexplored dimension of automotive cybersecurity by focusing on RF-level signal integrity. By developing a system that can detect and block unauthorized signal amplification, the project will contribute to preventing keyless vehicle thefts and strengthening automotive security standards.

Ultimately, the outcome of this research could influence **future design standards for keyless entry systems** and support the development of more secure, intelligent, and tamper-resistant automotive technologies.

Required Boards (PCBs) for this Project

A circuit board or module that can help with distinguishing RF signals (which aligns with our research topic of detecting tampered or amplified RF transmissions), here are **key design considerations** + **some existing modules** we would be examining and build upon.

What to look for / design criteria?

When we need to identify and distinguish authentic vs. amplified/tampered RF signals (e.g., from a key-fob around ~300 MHz), the detection board should ideally support the following features:

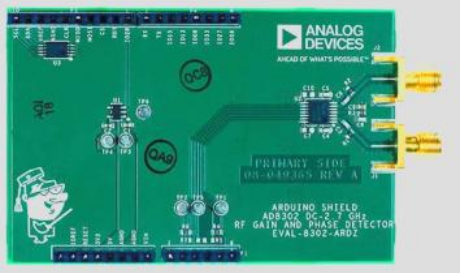
1. **Wide or targeted RF frequency range**, with good sensitivity.
    - Some RF detector ICs/modules monitor ~100 MHz up to several GHz. Ref: DigiKey
    - For our case (around 300 MHz), we'll want a design optimized around that band (and maybe harmonics / adjacent bands used by keyless systems).
2. **Signal parameter measurement** (not just presence/absence).
    - Amplitude (signal strength)
    - Rise time / envelope shape
    - Noise floor and interference
    - Possibly time-of-flight or delay/propagation (to detect relay/amplification)
    - Spectrum features (e.g., frequency shifts, distortion)
3. **Good PCB/RF layout practices**
    - Controlled impedance traces, short signal paths, proper ground planes. Ref: RF Power Detector
    - Use of RF connectors (e.g., SMA) for measurement or antenna input.
    - Shielding if needed.
4. **Output interface to your higher-level processing**
    - The detector board should output a measurable DC voltage or digital interface that we can feed into our MCU/firmware. Many RF detector ICs convert RF input into a proportional DC output. Ref: PCB RF power detector
    - Alternatively, integrate with an SDR (software-defined radio) or microcontroller + ADC for deeper feature extraction.
5. **Real-time or near-real-time capability**

- To detect when an amplified relay attack happens, we'll need a very low latency detection and ideally a blocking/mitigation mechanism (our proposal already mentions designing a circuit + firmware to neutralize unauthorized signals).
- Our hardware should thus support fast detection and trigger an action (blocking, jamming, alerting).

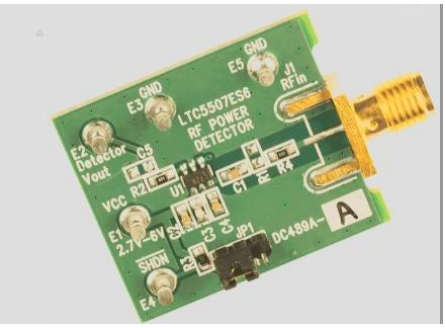
6. **Calibration and baseline of "authentic" transmissions**
   - To distinguish authentic from tampered signals, we'll need to profile genuine key-fob RF signals (strength, timing, modulation signature) and compare them to amplified/relayed versions.
   - The board might include memory or interface to store baseline signatures or feed into a machine learning model.
7. **Consider environmental and regulatory constraints**
   - The board must not itself interfere with legitimate transmissions or exceed regulatory limits (especially in Canada).
   - RF boards are susceptible to noise, spurious signals, multipath effects — our layout and firmware must account for this.

Some existing modules/boards that we can evaluate

Here are a set of product modules/boards that can either adopt directly for prototyping or use as inspiration for our custom board.

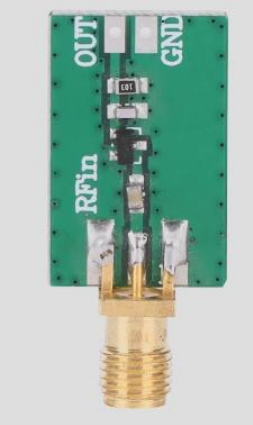


Analog Devices EVAL-AD8302-ARDZ Shield Board RF Detector – Cost $642.76, DigiKey Canada

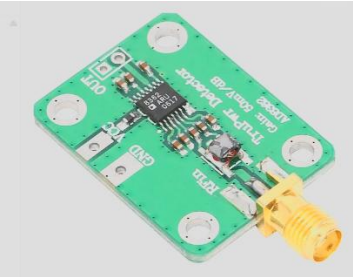


Analog Devices DC489A/DC1528A Demonstration Board RF Power Detector, $188.14

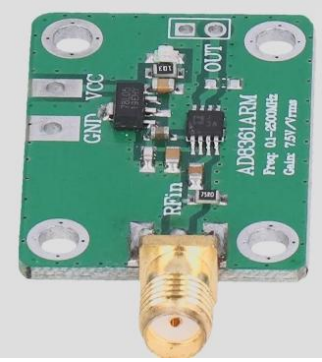
Dewin RF Detector Module Envelope Demodulation 0.1-3200 MHz, $7.88, Walmart.ca



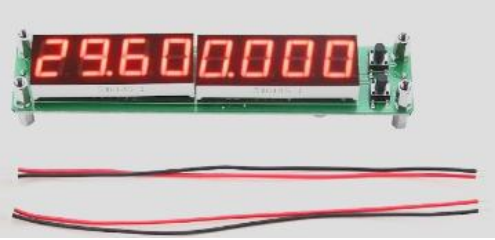
Estink Power Detector Board RF Detector Module Compact, $26.24, Walmart.ca



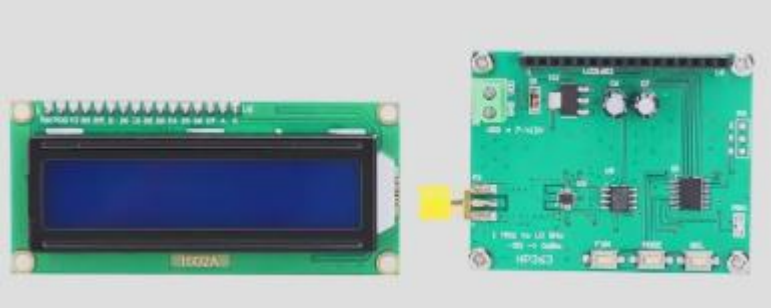
Frequency Detector Module RF Microwave AM Detection Board 0.1-2.5 GHz, $20.87, eBay - nbfyur98



PLJ-8LED-H Module RF Signal Tester 0.1-1000 MHz, $31.18, Amazon CA



RF Power Meter PCB 1 MHz-10 GHz Power Measurement Board, $49.92, Amazon CA



Mikroe RF Meter 3 Click, $40.45

Brief commentary on each:

- Analog Devices EVAL-AD8302-ARDZ Shield Board RF Detector: A high-precision evaluation board from Analog Devices for an RF detector IC (AD8302). Good for accurate amplitude/dc output measurement, ideal for prototyping detection of signal power differences.
- Analog Devices DC489A/DC1528A Demonstration Board RF Power Detector: Another professional board for RF power detection; great reference to understand layout, calibration, and measurement of RF input to DC output conversion.
- Dewin RF Detector Module Envelope Demodulation 0.1–3200 MHz: A relatively low-cost module that covers wide frequency band; you may need to check its performance around 300 MHz and sensitivity/linearity.
- Estink Power Detector Board RF Detector Module Compact: Another compact module, useful if you want a form-factor that can be embedded into your prototype vehicle I/O board.
- Frequency Detector Module RF Microwave AM Detection Board 0.1–2.5 GHz: Covers a broad band including your target; may be useful for detecting unexpected signals outside the normal key-fob band (to detect tampering or relay equipment).
- PLJ-8LED-H Module RF Signal Tester 0.1–1000 MHz: More of a visual indicator board (LEDs) — less precision, but useful for quick detection or demonstration.
- RF Power Meter PCB 1 MHz–10 GHz Power Measurement Board: A more general power-meter board; could be adapted for your purposes if you repurpose it to monitor around 300 MHz transmissions.
- Mikroe RF Meter 3 Click: A small embedded board ("click" format) that might integrate easily with a microcontroller platform; good for proof-of-concept or sensor integration.

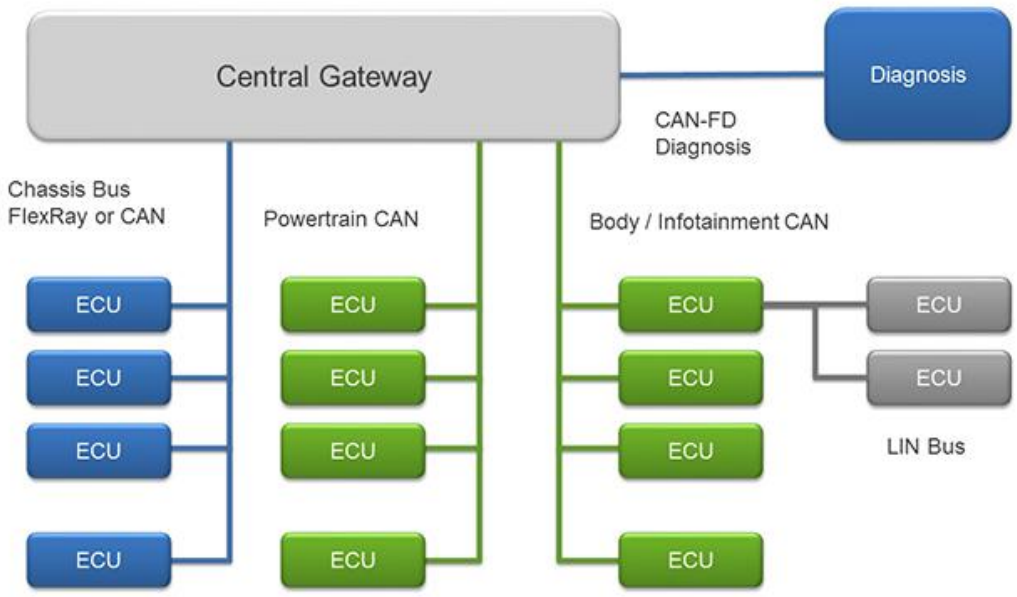
Recommendation for our research context

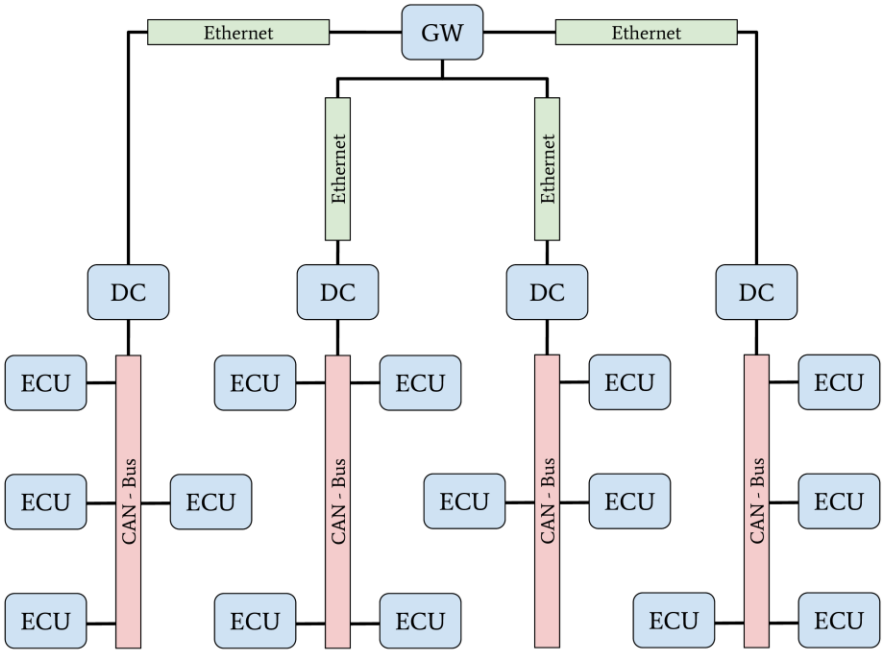
Given our goal (detect & block unauthorized signal amplification around ~300 MHz from keyless vehicle systems), here's how we would proceed:

- **Start with one of the evaluation boards** (like the AD8302 Eval-Board) to prototype our detection of RF signals, measure amplitude vs. baseline, test with genuine key-fob transmissions and amplified/relay versions.
- **Characterize genuine transmissions**: Use SDR, spectrum analyzer, and our detection board to capture key features: amplitude, rise/fall time, envelope, noise floor, legitimate range vs. extended range.
- **Simulate tampering/relay attack**: With amplification equipment (under legal/controlled lab setup) simulate how the key-fob signal changes (e.g., increased range, lower SNR, added delay) and capture those with our board.
- **Develop firmware/algorithm**: On our detection board (or on a microcontroller connected to it) implement thresholds, machine learning or statistical model to classify a signal as "authentic" vs "amplified/relayed".
- **Design custom board**: Based on lessons from the eval and modules, design a custom PCB optimized for your target (~300 MHz), integrated into vehicle hardware (possibly hidden within near the keyless entry receiver). Focus on layout (impedance, shielding), reliable detection, and interface to blocking mechanism (e.g., jam signal or shut down keyless module).
- **Integrate blocking/mitigation**: Once detection is robust, add the blocking hardware: this might include controlled jamming (if legal in your context), signal suppression, or alerting the vehicle ECU to reject the RF transmission.

Vehicle Network Components

Here are some useful diagrams showing vehicle network components and in-vehicle network architecture you can reference as visuals for understanding how ECUs, buses, and gateways connect in modern vehicles:





What these diagrams illustrate:

- **In-vehicle network topology with multiple bus systems** (CAN, LIN, FlexRay, MOST) showing how different ECUs are connected via shared buses and gateways.
- **Central gateway architecture** where various domain networks (powertrain, body, infotainment) connect through a central and domain gateways.
- **Domain-separated network structure** with a gateway (GW) that interconnects CAN domains using Ethernet backbone.
- **Automotive Ethernet and zonal architecture concepts** showing high-speed backbone connections.
- **Classic CAN bus connections** among ECUs and sensors illustrating how a simple vehicle network looks in practice.
- Another example of vehicle network layout across the car body for testing and diagnostics.

Typical components shown in such diagrams

- **ECUs (Electronic Control Units)** controlling functions such as engine, braking, body electronics
- **Communication buses** such as CAN, CAN-FD, LIN, FlexRay, MOST
- **Gateways** that connect heterogeneous networks and translate protocols Nexperia
- **Automotive Ethernet** as a high-speed backbone for advanced domains and ADAS systems Keysight
- **Domain controllers and central gateways** for secure segmentation of in-vehicle networks Automotive IQ

Context for how these relate

Modern vehicles are composed of tens to hundreds of ECUs communicating over **multiple network protocols**, each suited to different performance and cost requirements. CAN and LIN handle control tasks, FlexRay supports time-critical systems, MOST often supports multimedia, and Ethernet is increasingly used as a high-bandwidth backbone for advanced applications and zonal architectures. Messages flow through **Gateway modules** that bridge these networks and help enforce security policies. Nexperia+1