Authenticating CAN Message Origin

A Deep Dive on CAN Spoofing Detection Using Power Fingerprints

Ken Broden

University of Minnesota Morris

November 13, 2025

Introduction to the CAN Bus

- Controller Area Network
- Connects all vehicle ECUs
- Industry standard
- Reliable, real-time data exchange

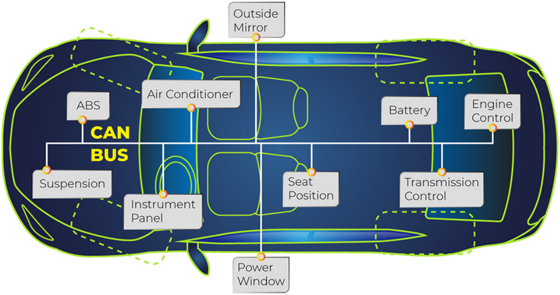


Figure: CAN network overlayed on a vehicle.

Motivation & Scope

Figure: Jeep hack by Miller and Valasek.

- Modern vehicles: many ECUs, high connectivity, safety-critical behavior.
- CAN: reliable and efficient, but designed without security.
- Research Goal: Add security without increasing latency or changing CAN protocol.

Research Question & Contributions

- **Question**: Can CAN messages be authenticated using physical-layer data without changing the protocol?
- **Proposed solution: CANOA** - Controller Area Network Origin Authentication
  - Uses each ECU's unique power fingerprint
  - Verifies message origin without added delay

Outline

1. Introduction
2. Background: How CAN Works
3. Threat Model & Attack Example
4. CANOA: Power Fingerprint Authentication
5. Algorithms
6. Evaluation & Results
7. Limitations & Edge Cases
8. Conclusion

Introduction to the CAN Bus

- Two-wire shared bus
- Broadcast-based communication

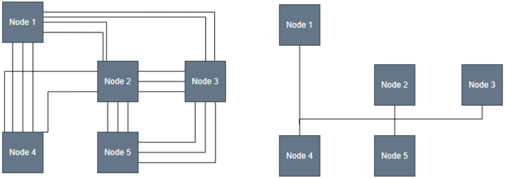


Figure: Comparison of ECU communication with and without a CAN bus

Physical Layer: Twisted-Pair Wiring

- Two wires: **CAN H** (high) and **CAN L** (low)
- Twisted pair design reduces noise and interference
- All ECUs share the same two-wire bus

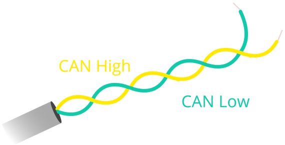


Figure: Twisted-pair wiring for CAN H and CAN L.

CAN Network Topology

- ECUs connected in parallel on CAN H and CAN L
- All messages are broadcast to every node

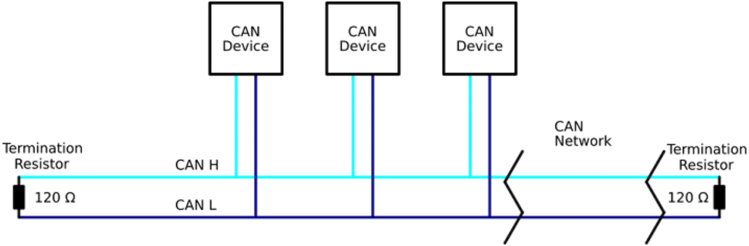


Figure: Example of ECUs sharing the same CAN bus.

Differential Signaling on CAN

- Data = voltage difference between CAN H and CAN L
- Recessive: both ≈ 2.5 V
- Dominant: CAN H ≈ 3.5 V, CAN L ≈ 1.5 V
- Dominant overrides recessive

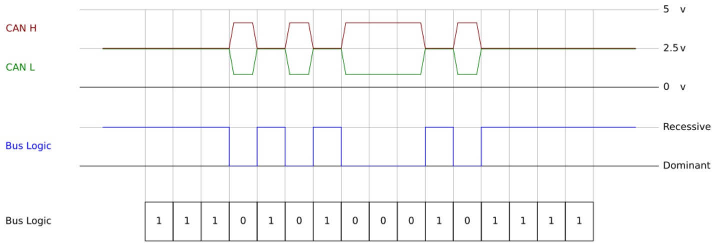


Figure: Voltage levels for recessive and dominant bits.

CAN Frame & Arbitration

- Frame = ID + control + data
- ID defines message type
- Lower ID = higher priority
- Bitwise arbitration prevents collisions

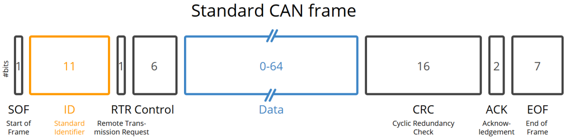


Figure: Simplified CAN data frame.

CAN Bus Arbitration

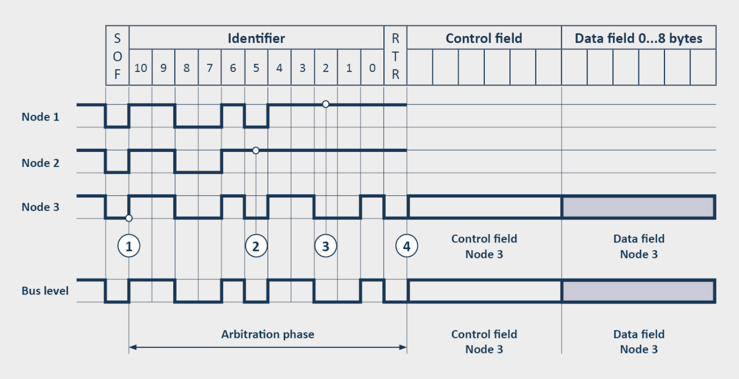


Figure: Arbitration by Dominant (0) and Recessive (1) Bits

- All ECUs start sending simultaneously.
- The ECU with the lowest identifier (more leading 0s) wins and continues transmission.

Security Gaps (Why Extra Protection Is Needed)

- No built-in authentication or encryption.
- Broadcast + ID-based arbitration ⇒ a single sender is heard by all nodes.
- Spoofed low-ID frames can win arbitration and effectively control many ECUs.

Message Spoofing & Injection

- Attacker reuses target ECU's ID to inject fake frames.
- Arbitration can help attacker deliver high-priority frames first.
- Safety, reliability, and privacy risks.

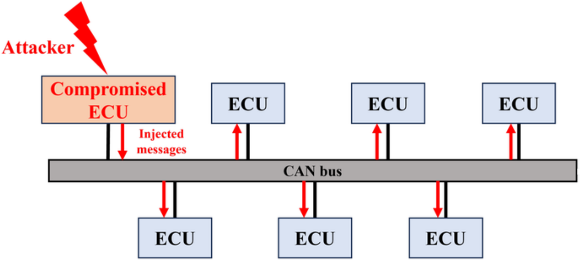


Figure: Injected messages by a compromised ECU

Core Idea & Rationale

- Each ECU's hardware draws a distinct current profile during transmission.
- Measure power usage ⇒ build **power fingerprint** per ECU.
- **Benefit:** physical-layer auth; no cryptographic overhead or CAN changes.

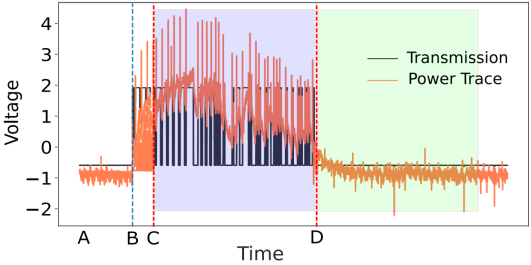


Figure: Power trace of ECU during transmission, and at idle.

System Setup Hardware

- Deployment concept: sensor placement, monitoring unit, CAN connection.

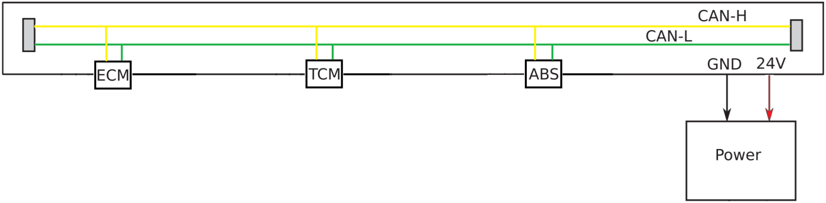


Figure: Three node CAN with power connection.

System Setup Hardware

- Deployment concept: sensor placement, monitoring unit, CAN connection.

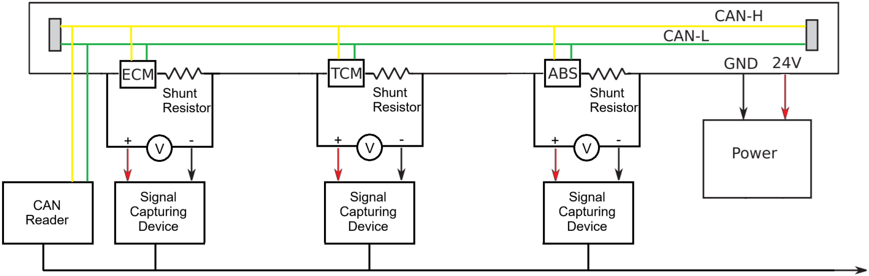
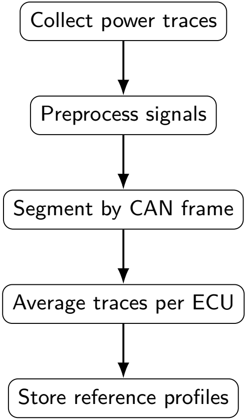


Figure: CANOA hardware implementation.

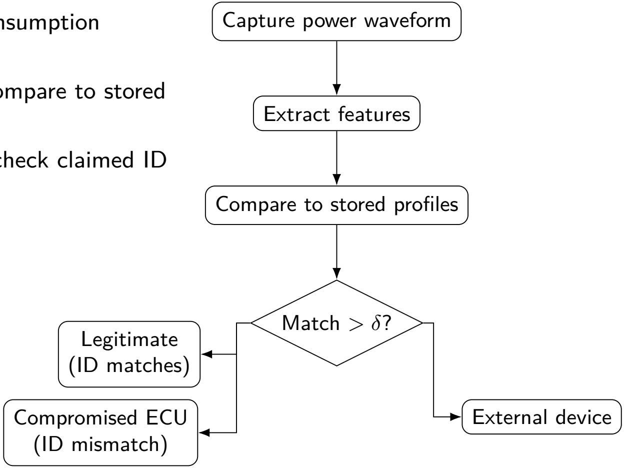
Algorithm 1: Reference Signal Generation



- Collect ECU power traces during message transmission.
- Clean and preprocess the raw signals.
- Segment the traces by individual CAN frames.
- Average multiple samples to form a stable reference for each ECU.
- Store the profiles for future comparison during verification.

Algorithm 2: Online Verification (CANOA)

- Sample ECU power consumption during transmission.
- Extract features and compare to stored profiles.
- If highest match $> \delta$, check claimed ID vs matched ECU.



Experimental Setup

- Lab bench + real vehicle (truck) environments.
- Metrics: detection rate, latency, robustness to noise/conditions.

Figure: Sterling Acterra heavy duty truck

Key Findings

- **Lab Prototype:**
  - 4 simulated ECUs on 125 kbps CAN bus.
  - ≈1,000 spoofed frames injected - all detected.
  - Average per-message verification latency < 0.05 ms
- **Truck Test:**
  - 5 real ECUs on 250 kbps bus (ECM, TCM, ABS, BCM, Cluster).
  - ≈100,000 messages analyzed from normal operation.
  - ≈99.9% authentication accuracy, $<$0.05 ms latency.

What CANOA Does Not Cover

- Legitimate-but-compromised ECU (correct fingerprint, malicious intent)
    - Control that ECU's function maliciously
    - DoS attack / bus flooding
- Sensitivity to power noise or hardware changes (requires recalibration)

Future Considerations for CANOA

- **Simpler Hardware:** Explore measuring total system power instead of each ECU.
- **Reliability:** Study how temperature, noise, and ECU aging affect accuracy.
- **Lower Cost:** Test lower sampling rates and simpler sensors for practicality.
- **Extended Research:** Combine power data with other signals (e.g., acoustic) for stronger authentication.

Takeaways

- Modern vehicles need reliable message authentication - the CAN protocol alone leaves security gaps.
- CANOA provides a practical solution by verifying message origin without altering the existing CAN framework.
- Most effective as part of a layered defense, adding a valuable physical layer to vehicle cybersecurity.

References

Charlie Miller and Chris Valasek. 2015. *Remote Exploitation of an Unaltered Passenger Vehicle*. Technical Report. IOActive, Seattle, WA, USA. `https://ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf`

Shailja Thakur, Carlos Moreno, and Sebastian Fischmeister. 2024. CANOA: CAN Origin Authentication through Power Side-channel Monitoring. *ACM Trans. Cyber-Phys. Syst.* 8, 2, Article 13 (May 2024), 30 pages. doi:`10.1145/3571288`

Thank you!