Manuscript submitted to *Security and Safety*, For Peer Review Only, Vol. x, xxxxxxx (2023)
https://doi.org/10.1051/sands/xxxxxxx
sands.edpsciences.org

Research Article OPEN ACCESS

Section Category

Physical-Layer Exploits on EV Chargers: Authentication and Systemic Protocol Weaknesses

Hetian Shi[1], Shangru Song[1], Yi He[2], Zhenhao Tian[1], Jianwei Zhuge[13*], and Jian Mao[4]

[1] *Tsinghua University, 100084, China*
[2] *Wuhan university, 430072, China*
[3] *Zhongguancun Laboratory, 100094, China*
[4] *Beihang University, 100191, China*

Received: xx xxxxx 2022 / Revised: xx xxxxx 2022 / Accepted: xx xxxxx 2022 / Published online: xx xxxxx 2022

Abstract The proliferation of electric vehicles in recent years has significantly expanded the charging infrastructure while introducing new security risks to both vehicles and chargers. In this paper, we investigate the security of major charging protocols, including SAE J1772, CCS, IEC 61851, GB/T 20234, and NACS, and uncover new physical signal spoofing attacks in their authentication mechanisms. By inserting a compact malicious device into the charger connector, attackers can inject fraudulent signals to disrupt the charging process, resulting in denial-of-service, vehicle-induced charger lockout, and damage to the chargers or the vehicle's charge management system. To demonstrate the feasibility of our attacks, we propose PORTulator, a proof-of-concept (PoC) attack hardware, including a charger gun plugin device for injecting physical signals and a wireless controller for remote manipulation. By evaluating PORTulator on multiple real-world chargers, we identify 7 charging standards used by 20 charger piles that are vulnerable to our attacks. These attack primitives are not merely protocol flaws, but practical cyber-physical threats that can be leveraged for service disruption, extortion, and targeted sabotage in public or fleet-dependent charging environments. The root cause is that chargers use simple physical signals for authentication and control, making them easily spoofed by attackers. To address this issue, we propose enhancing authentication circuits by integrating non-resistive memory components and utilizing dynamic high-frequency Pulse Width Modulation (PWM) signals to counter such physical signal spoofing attacks.

Keywords Charging piles, Charging ports, Spoofing signal, Hardware Reverse Engineering

Citation Shi et al.. Physical-Layer Exploits on EV Chargers: Authentication and Systemic Protocol Weaknesses. Security and Safety 2023; **x**: xxxxxxx. https://doi.org/10.1051/sands/xxxxxxx

1 Introduction

The widespread adoption of EVs represents a transformative shift towards sustainable transportation, addressing environmental concerns and reducing dependence on fossil fuels. Meanwhile, new security issues [1–3] are emerging within the EV charging infrastructure. Unfortunately, as more EV chargers are deployed in cities, they become increasingly attractive targets for cyberattacks. Moreover, the complexity and diverse range of charging standards open the door to numerous vulnerabilities that could threaten both user safety and the stability of critical charging infrastructures [4]. These weaknesses are not only reliability concerns, but also create practical opportunities for adversaries to impose asymmetric disruption on charging-network operators and EV users. In real deployments, attacks on charging availability or charging-state integrity can translate into financial loss, operational disruption, reputational damage, and even coercive leverage in public or fleet-dependent charging scenarios.

[R4-3] Add real-world attacker incentives.

* Corresponding author (email: zhugejw@tsinghua.edu.cn)

This provisional PDF is the accepted version. The article should be cited as: Security and Safety doi: 10.1051/sands/2026012

Existing works [5–7] mostly focus on remote attacks. For instance, the Brokenwire attack [5] can disrupt the Combined Charging System (CCS) charging process by performing remote electromagnetic interference on the charger's programmable logic controller (PLC) to terminate the charging session. While Nasr et al. [7] and Vailoces et al. [8] both analyze vulnerabilities in the backend of electric vehicle supply equipment (EVSE) systems, including charge management platforms and network-level authentication, little attention has been paid to the physical-layer signaling protocols and port-level logic at the EV charger interface.

In this work, we investigate local attacks on charger piles and identify new common physical attack vectors that can exploit the weaknesses in the authentication process of several major charging standards. We demonstrate practicable physical signal injection attacks on various real-world charger pipes. By planting a small concealed hardware plugin onto the charging guns, attackers can inject control signals into the various ports of the guns. Specifically, by manipulating different ports with specific physical signals, attackers can launch: (1) Denial-of-service (DoS) attacks disrupting charging via Charging Confirmation (CC) / Control Pilot (CP) port manipulation; (2) Deadlock attacks spoofing impedance on the CC port, which can lockout the charging gun; and (3) PWM/CAN Bus signal injection attacks that can damage the EV battery, overloading the charging system, or inject malicious CAN Bus message to further exploiting the inner systems of vehicles. We prototype an attack hardware called PORTulator, which can be seamlessly integrated into the charger guns' ports and perform physical signal injection attacks. Unlike [9], which only showed a simple demo of authentication issues, our work is the first to fully study and exploit state forgery problems in several EV charging protocols. We show that attackers can tamper with the physical authentication process and then send fake CAN messages to the vehicle, which can bypass battery safety protections and cause overcharging. We evaluate PORTulator on several real-world chargers and identify that 7 charging standards used by 20 charger piles are vulnerable to our attacks. Finally, we propose defensive strategies to mitigate these vulnerabilities, offering solutions that enhance the cybersecurity of EVSE systems. By integrating non-resistive memory components and utilizing dynamic high-frequency Pulse Width Modulation (PWM) power in existing charging authentication processes, the impedance is changed from fixed values to changeable values that are infeasible to be forged by attackers.

Here are the contributions of our work:

- We first identify critical weaknesses in the authentication mechanisms of multiple EV charging standards and show that they enable not only charging-process DoS, charging-port lockout, and unsafe charging-state manipulation, but also, under architecture-dependent conditions, escalation toward vehicle-side CAN-domain interference. These weaknesses constitute practical cyber-physical threats with clear implications for service disruption, extortion, and targeted sabotage.
- We develop PORTulator, an attack suite that integrates a microcontroller unit (MCU), flexible printed circuit (FPC), and wireless communication, enabling covert connection to different charging standards and remote manipulation of vehicle charging port states for various attacks.
- We test PORTulator against multiple mainstream charging gun standards, demonstrating its practical effectiveness in real-world scenarios and providing three comprehensive case studies to highlight significant threats to vehicle charging safety.
- To address these vulnerabilities, we propose a defensive mechanism and validate it with real-world prototypes. Experimental results show that it can effectively prevent physical signal injection attacks.

2 Preliminaries

Electric-vehicle (EV) charging relies on a compact set of physical interfaces and simple analog-level checks at the charge port. In this paper, we focus on the low-level signaling and port logic (e.g., CC/PP/CP and, for fast charging, CC1/CC2) that jointly determine insertion state, authorization, and permissible charge current. These physical signals are fundamental to safety (e.g., electromechanical locks) and to the negotiation that precedes power transfer.

2.1 Charging Process and Control Signals

After a charging gun mates with the vehicle inlet, the vehicle samples the **Charging Confirmation (CC)** and related pilot lines to infer connection and user intent; once a valid insertion state is observed,

the vehicle typically engages an electromechanical lock. The **Control Pilot (CP)** line then carries a 1 kHz PWM signal whose duty cycle encodes the allowed charging current and operational mode (e.g., *standby*, *charging*, *ventilation required*, *error*) in IEC-style standards [10]. Figure 1 summarizes this flow.

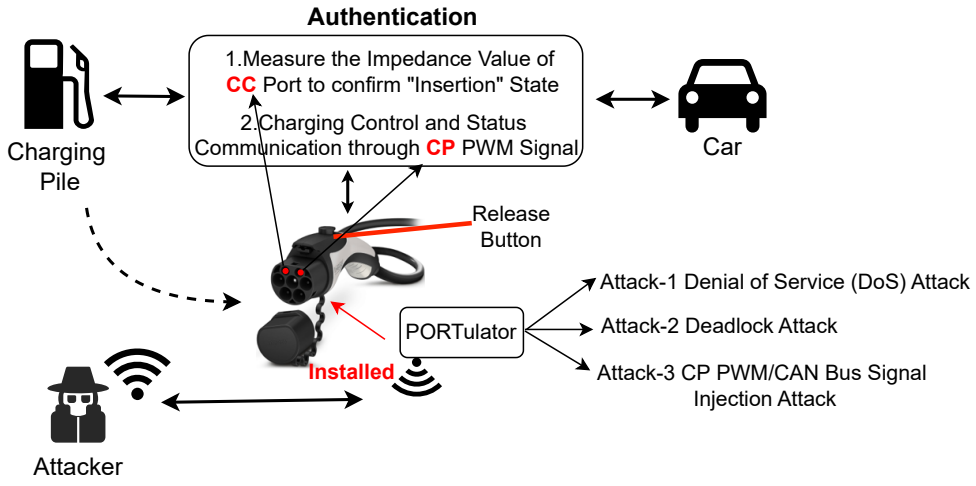


Figure 1: Overview of PORTulator Attack Vectors on EV Charging Infrastructure

Many charging standards implement the initial insertion/authentication using simple analog thresholds (voltage or impedance) on the CC/PP pins (see Table 1). After the analog check succeeds, higher-level digital or networked authentication (if present) and power negotiation occur before current is enabled.

2.2 Observed Weak Signals

We observed two practical weaknesses that are central to our attack surface:

Unauthenticated Wireless "Open-lid" Commands. Some guns emit a fixed radio command that opens the charge-port lid. We captured such a waveform from a NACS-compliant gun (HackRF One + GQRX) and, in replay tests using URH, successfully opened several vehicles' charge ports (Tesla Model S/Y, VW ID.4). The command format is short and reused across deployments, making it trivial to replay with low-cost SDR hardware.

Analog Reliance for CC/CP Authentication. The CC/CP handshake frequently reduces to verifying resistor/voltage ranges or PWM duty cycles rather than cryptographic exchange. Because the vehicle's state machine triggers mechanical locking and enables power based on these analog conditions, an adversary that forges the expected impedance or PWM patterns can induce unauthorized state transitions (DoS, deadlock, or manipulated current limits).

2.3 Safety Measures

Electromechanical locks and in-session monitoring are standard safety measures across GB/T, IEC, SAE J1772, NACS and CCS families [11–13]. These mechanisms are designed to prevent accidental disconnection and to ensure safe current transfer; however, when the authentication decision depends only on static analog signatures, these safety mechanisms can be abused or subverted by forged signals (see §3.2 for details).

3 Overview

3.1 Motivation

The rapid global adoption of electric vehicles (EVs) has driven the large-scale deployment of diverse charging infrastructures, bringing new security challenges to the physical and signaling layers

of EV–charger communication [5]. Recent work revealed a weak authentication flaw in the GB/T 20234.2 standard [9], where resistance manipulation on the Charging Confirmation (CC) line can cause unauthorized state transitions or deadlocks. Yet, the broader impact of such vulnerabilities remains unclear across different charging standards. In this study, we empirically analyze multiple EV charging protocols to determine whether signal-level spoofing can be generalized across standards and whether these attacks can escalate from simple denial-of-service to deeper control over the EV's charging management system.

3.2 Weak Authentication Vulnerabilities in Charging Ports

Authentication mechanisms in EV charging protocols are designed to prevent unauthorized access to vehicle charging functions. However, our investigation reveals that several widely adopted standards rely on weak signal level authentication [14–16], where charging state transitions are determined by analog parameters such as port impedance or PWM duty cycles, without any cryptographic validation. This architectural assumption leaves room for adversaries to spoof authentication signals and gain unauthorized control over the charging process. Figure 2 illustrates a typical falsified signal attack that exploits this weakness.

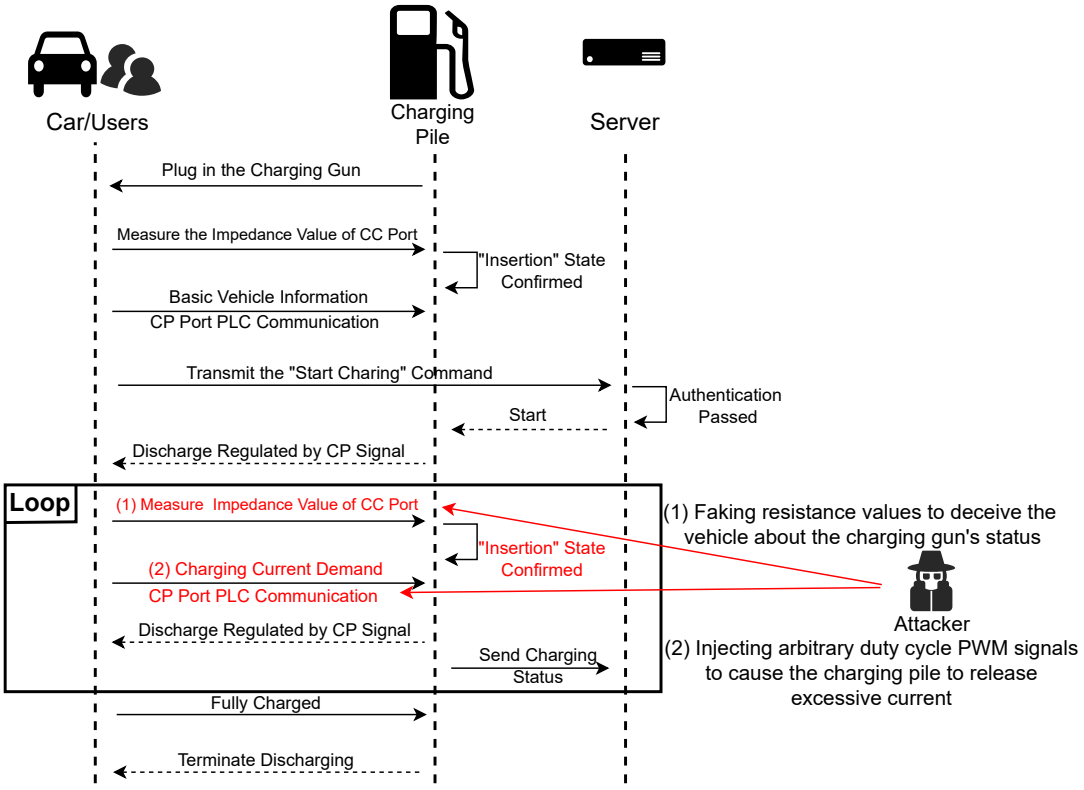
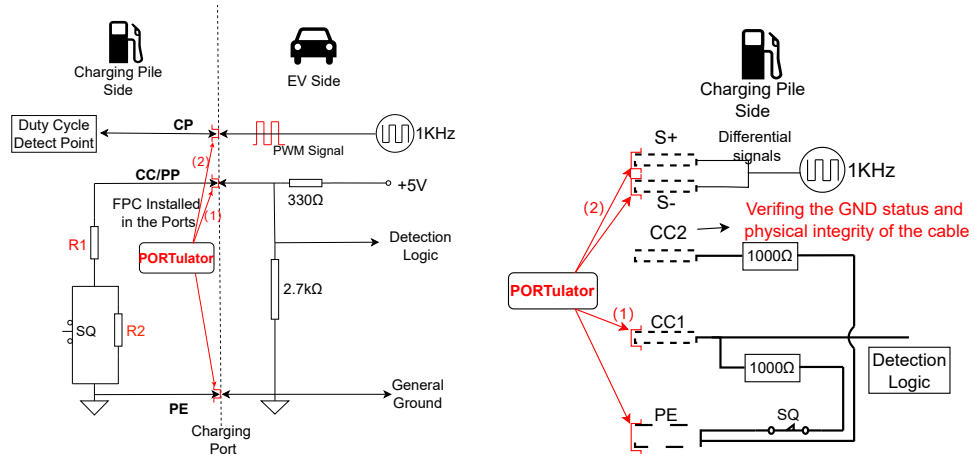


Figure 2: Falsified Signal Attack Exploiting Weak Authentication in Charging Protocols

To explore this vulnerability, we begin by reverse engineering the internal signal circuits of several representative charging guns. In an initial study of a GB/T AC charging gun, we use a multimeter to probe the impedance of the CC line and identify an unexpectedly simple configuration consisting of only two resistors and a mechanical travel switch. Although this demonstrates the feasibility of spoofing CC signals by manipulating resistor values, we also note the risk of signal coupling between ports. To better understand the design, we disassemble the gun and confirm that the authentication logic relies purely on passive resistance and mechanical actuation, with no built-in tamper detection.

Since many commercial charging guns employ anti-tamper designs that hinder physical disassembly, we developed PORTulator, a non-invasive port analysis tool capable of automatically identifying internal



(a) Slow Charging Gun Authentication Circuit (b) Fast Charging Gun Authentication Circuit

Figure 3: Comparison of Slow and Fast Charging Gun Authentication Circuits

electrical characteristics. By interfacing with multiple charging gun ports, PORTulator can assess port isolation, impedance values, and the presence of memory components such as capacitors or inductors, without opening the casing. This allows us to extract authentication logic from devices across multiple standards in a repeatable and scalable manner.

Figure 3 shows the typical internal signal circuits for slow and fast charging guns, which were mapped using our automated method. The wiring differs across charge modes, the *authentication primitive* is similar: the charger infers connection and readiness states from *analog thresholds* on low-voltage lines. In AC/slow charging (Figure 3a), the CP line carries a 1 kHz PWM pilot and the state is primarily determined by a resistor-divider response. In DC/fast charging (Figure 3b), implementations typically introduce dual CC paths (e.g., CC1/CC2) and may expose additional communication conductors for higher-layer control; nevertheless, the initial trust decision still depends on simple analog conditions (impedance/voltage windows) before any higher-layer protocol exchange.

R2: clarify AC/DC differences but similar authentication logic.

Building on this insight, we designed a signal spoofing attack targeting these weak authentication mechanisms. The attack involves mimicking the electrical signatures that represent various charging states. For example, as summarized in Table 1, changing the resistance value on the CC line can simulate events such as plug insertion, button press, or user confirmation. By replicating these states, an attacker can deceive the charging pile into initiating or continuing a charging session without authorization.

To construct these spoofed signals, we first used PORTulator to capture reference waveforms and parameter ranges during normal charging sessions. This included measuring resistance transitions, PWM frequencies, and voltage thresholds under different operational states. Based on this data, we generated counterfeit signals using a programmable MCU that emulates the behavior of a legitimate EV-side interface. These signals are then injected into the CC or CP ports at specific phases of the charging handshake to trigger unauthorized transitions.

Since the charging pile relies solely on analog signal conditions for authentication, it is unable to distinguish between genuine and spoofed interactions. As a result, the attacker can initiate, manipulate, or deadlock the charging process, even without any access to cryptographic credentials or prior pairing with the vehicle.

3.3 Formal Model of Authentication & Attack Conditions

We model EV–charger authentication as a cyber-physical finite-state system. Let $S = \{s_0, s_1, s_2, s_3\}$ denote the states $\{$*disconnected*, *connected*, *ready*, *charging*$\}$. The charger samples the control-circuit voltage $V_{cc}(t)$ and uses threshold ranges $\mathcal{V}_{ij}$ to decide transitions $s_i \to s_j$:

$$V_{cc}(t) \in \mathcal{V}_{ij} \quad \Longrightarrow \quad s_i \to s_j.$$

The physical pilot voltage follows the voltage-divider model

$$V_{cc}(t) = V_{ref} \cdot \frac{R_{EV}(t)}{R_{EVSE} + R_{EV}(t)},$$

where V_{ref} is the EVSE reference voltage, R_{EVSE} is the charger-side pull resistance, and $R_{EV}(t)$ is the vehicle-side equivalent resistance. (Full formal derivations and noise/robustness analysis are omitted here for brevity; key implications are discussed in §4 and §4.2.)

3.4 Threat Model

We consider an adversary with brief, opportunistic physical access to public charging equipment (e.g., parking lots or semi-supervised stations). The adversary can covertly attach a small, dormant device to a charging gun that is later remotely triggered to inject or modify CC/CP signals. We assume no firmware modification, **no long-term persistence** on backend systems, and no prior cryptographic credentials. The attacker's goal is limited to forging port-state transitions (e.g., induce DoS, deadlock, or alter charging parameters); on some interfaces (e.g., GB/T 20234.3, NACS), exposed wiring may allow escalation to in-vehicle bus access (e.g., CAN), but this is not assumed for all targets. We consider not only opportunistic attackers seeking direct extortion, but also sabotage-oriented adversaries aiming to disrupt charging availability, damage operator reputation, or target fleet users whose operations critically depend on timely charging. In addition, where connector-side communication paths expose a reachable in-vehicle bus, the attack surface may be attractive to more capable adversaries seeking deeper functional compromise rather than mere service interruption.

4 PORTulator Design

To verify if the chargers are vulnerable to physical signal injection attacks, we propose PORTulator, a customize hardware platform based on the RP2040 Microcontroller Unit (MCU), designed to uncover and exploit signal-level vulnerabilities in EV charging infrastructures. This device enables remote and precise manipulation of physical-layer communication between electric vehicles and charging piles, supporting real-world spoofing and injection attacks.

4.1 Hardware Design

The core of PORTulator is a compact, modular spoofing device—PORTulator —built to physically interface with the CC and CP lines of standard EV charging guns. As shown in Figure 4, the system is powered by an RP2040 MCU, chosen for its real-time control capabilities, low-latency GPIO access, and flexible ADC/DAC integration.

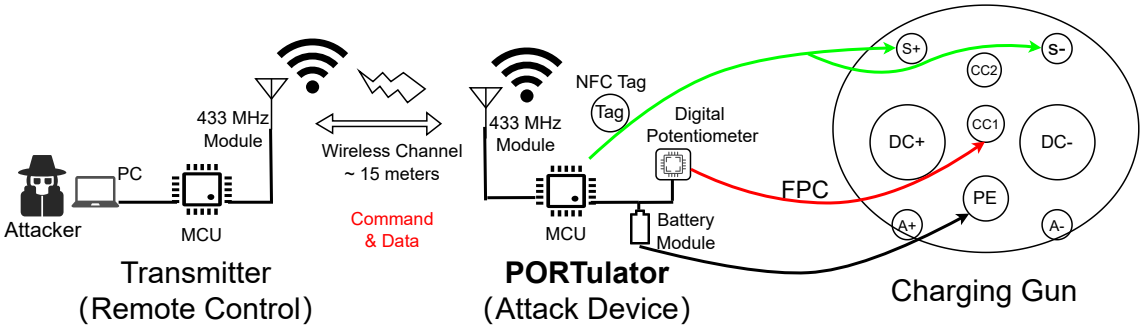


Figure 4: Design of PORTulator for Resistor Spoofing & Signal Injection

The PCB is designed to interface directly with both analog signaling pins (CC/CP) and digital monitoring subsystems. A programmable potentiometer (AD5160 module) is included to emulate

impedance-based logic states on the CC line, while a PWM-capable GPIO output pin synthesizes the CP signal to reflect various charging states. To allow for remote-controlled behavior, the hardware integrates a 433 MHz wireless receiver (GC433-TC007) that accepts over-the-air commands from an Arduino-based controller. This setup enables dynamic payload delivery, such as adjusting resistance values or toggling CP duty cycles, effectively changing the perceived EV state in real-time.

The physical device is encapsulated in a modified charging gun shell. Specifically, a thin custom cable is routed through the charging gun to the CC pin, internally connected to a pre-configured resistor, and routed through an insulating sleeve to avoid interfering with normal charging pile operations. A small metal ring is used to stabilize the CC contact position. This modification is minimally intrusive, does not affect standard charging under normal conditions, and is nearly invisible from the outside, making the attack device covert and practical for deployment in semi-public scenarios. In addition, the compact design enables rapid installation: the entire module can be integrated into a fake adapter or portable testing tool and clipped onto the target charging gun in under 90 seconds, minimizing the attacker's exposure time on-site.

Figure 5 shows the physical construction of the prototype. All components used are off-the-shelf and reproducible: the microcontroller board (RP2040), AD5160 potentiometer, GC433 wireless module, and the modified charging gun enclosure. The PORTulator is implemented as a ring-shaped PCB, as shown in Figure 5, the attacker disguises the device as part of the charger and mounts it onto the cable of the charging gun. PORTulator's hardware setup and open-sourced code is provided at: https://github.com/Moriartysherry/ev-charging-station-security.

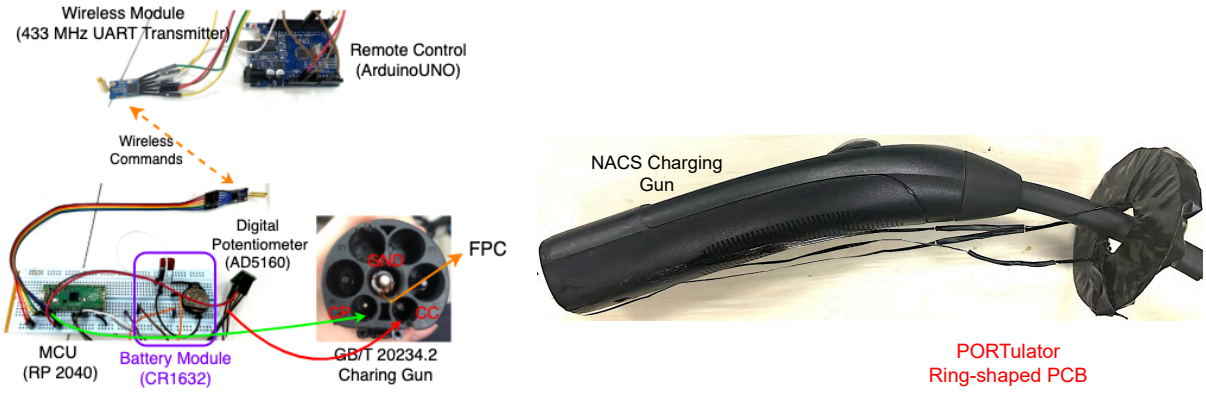
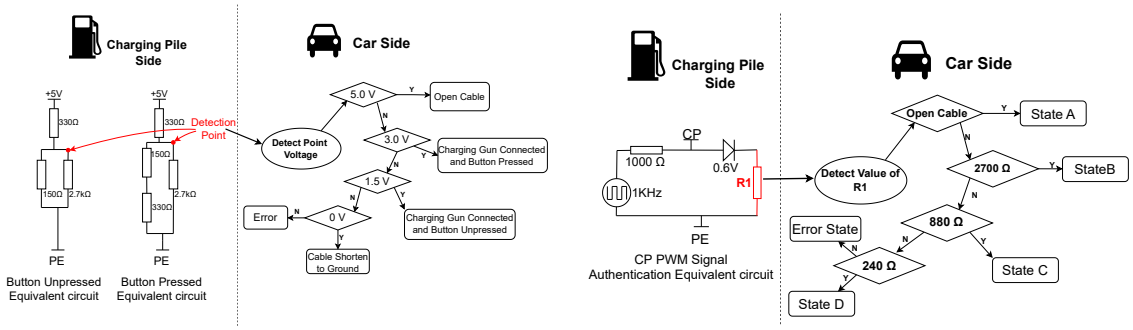


Figure 5: Physical Prototype of the PORTulator Attack Device

4.2 Signal Interpretation & Injection Principles

The design of PORTulator is grounded in the signal-level understanding of EV charging protocols, particularly the logic interpretation on CC and CP lines. Our system mimics legitimate interactions by matching impedance and PWM behaviors expected during the communication phase.

- **Impedance-Based Logic for CC Port Status.** The CC pin voltage is derived from a resistive divider between the EV's internal pull-down resistor and a fixed resistor inside the charging gun, typically connected through a travel switch linked to the trigger button. As illustrated in Figure 6a, the vehicle interprets the measured CC voltage to infer the connection state: about 5 V denotes an open cable, ∼3 V indicates the gun is connected, and the button is pressed, ∼1.5 V corresponds to connected but unpressed, and 0 V represents a short or fault condition.
- **PWM Signal-Based Logic for CP Port Status.** The CP line determines the vehicle's connection and charging state through an equivalent resistance R_1 between the transistor and ground (Figure 6b). In the default unconnected state (State A), no resistor is present, and the charger interprets this as "cable not connected." When physically connected (State B), the EV applies a 2.74 kΩ pull-down resistor, indicating presence without charging intent. Once ready to charge (State C), a 1.3 kΩ resistor



(a) Impedance-Based Logic for CC Port Status (b) PWM Signal-Based Logic for CP Port Status

Figure 6: Parameter Values and Logical State Determinations at the CC Port (a) and CP Port (b) of EV Charging Gun

is added in parallel, producing an effective 880 Ω and authorizing charging. Only in this state does the EV modulate the CP line with a 1 kHz PWM signal, whose duty cycle encodes the allowable charging current (e.g., 50% for 32 A, 85% for 51 A). Some implementations further use 240 Ω to indicate DC charging with forced ventilation. Any deviation from these expected values, such as undefined or shortened configurations, leads to a fault state (State D).

To ensure compatibility across various charging standards, we systematically reproduced the expected impedance values used to signal connection states. As shown in Table 1, PORTulator precisely emulates these reference resistances, with minimal deviation, to maximize spoofing success across a range of charging standards. These deviations do not trigger detection in practice because most EVSE/EV implementations infer states via **analog signal thresholds** (voltage windows) rather than exact resistance matching. Concretely, the CC/CP network forms a resistor-divider, and the controller (or an analog comparator) maps the measured node voltage (V_{sig}) to a discrete state using **predefined threshold bands** ($[V_1, V_2), [V_2, V_3), \dots$).

R2: explain tolerance/ guard-band based acceptance.

Standard	Unpressed Status (Expected Impedance)	Real Impedance (Deviation Ω)	Pressed Status (Expected Impedance)	Real Impedance (Deviation Ω)
SAE J1772	480 Ω	487 (+1.5%)	150 Ω	145 (-3.3%)
CCS I	480 Ω	487 (+1.5%)	150 Ω	145 (-3.3%)
IEC 61851	1030 Ω	1027 (-0.3%)	760 Ω	768 (+1.1%)
CCS II	1030 Ω	1027 (-0.3%)	760 Ω	768 (+1.1%)
NACS	460 Ω	466 (+1.3%)	400 Ω	390 (-2.5%)
GB/T 20234.2	220 Ω	210 (-4.5%)	3520 Ω	3511 (-0.3%)
GB/T 20234.3	0 Ω	0 (0%)	1000 Ω	1003 (+0.3%)

Table 1: Comparison of Expected and Spoofed Impedance Values Across Different Charging Standards

Due to component tolerances, ADC quantization, cable/contact resistance, temperature drift, and aging, real systems intentionally allocate a non-trivial *guard band* between thresholds so that normal variation does not cause state flapping. As a result, a small resistance deviation ΔR only perturbs the measured signal voltage by

$$\Delta V \approx \frac{\partial V_{\text{sig}}}{\partial R}\,\Delta R,$$

and as long as the perturbed voltage remains within the same threshold band, the state decision is unchanged, and no anomaly is raised. In our calibration, we verified that the deviations reported in Table 1 keep V_{sig} inside the intended threshold window for each corresponding state, which explains why these non-zero impedance differences do not trigger rejection while still enabling reliable spoofing across both AC and DC charging scenarios. This calibration enhances cross-standard reliability and enables consistent behavior in both AC and DC charging scenarios. This calibration enhances cross-standard reliability and enables consistent behavior in both AC and DC charging scenarios.

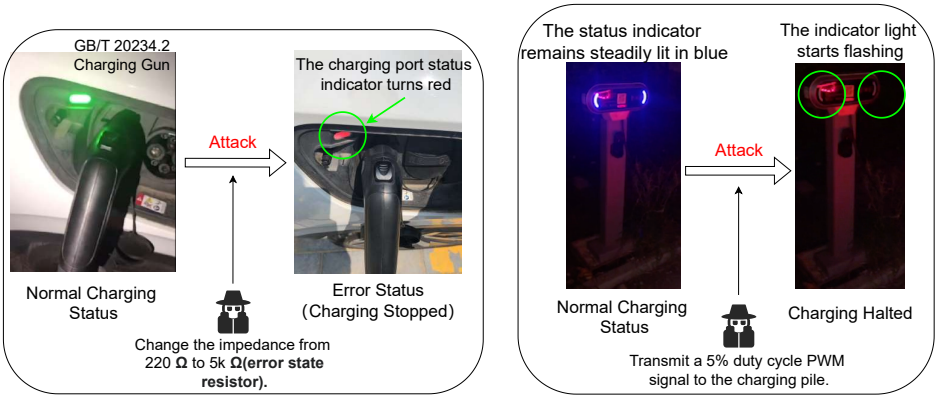
5 Evaluation

In this section, we evaluate the effectiveness of PORTulator across three key physical-layer attack scenarios: (1) inducing Denial-of-Service (DoS) conditions by manipulating the CC and CP lines, (2) spoofing resistor values to deadlock the charging gun in ransom-style attacks, and (3) injecting malicious PWM signals to manipulate charging behavior. We further explore the potential for higher-layer CAN Bus injection via the charging interface.

Specifically, PORTulator successfully executed all three attacks across seven EV models and six major charging standards in Table 2.

5.1 Case I: DoS Attack

During charging, EVs and charging piles continuously monitor the physical state of the charging connector to ensure safe operation under high-voltage and high-current conditions. Events such as abnormal impedance changes, improper insertion, or communication-state inconsistencies are treated as safety-critical faults and will immediately terminate or suspend power delivery. While this mechanism is designed for protection, it also creates an opportunity for adversaries to trigger charger-side or vehicle-side fail-safe logic intentionally.



(a) DoS on CC to Disrupt Charging Process (b) DoS on CP to Control Charging State

Figure 7: DoS Attacks on CC and CP Lines in EV Charging Systems

As shown in Figure 7a, our attack leverages this safety mechanism by exploiting the capabilities of PORTulator, as detailed in § 4. Specifically, attackers can remotely alter the CC line impedance to abnormal values, for instance, reducing it to 0 Ω or increasing it to simulate a disconnected state. This results in the charging pile immediately terminating the session. We validated this behavior on multiple vehicles, including the Volkswagen ID.4 and Tesla Model S. By pre-installing PORTulator on public charging piles, an attacker could remotely issue commands across various charging standards to launch broad DoS attacks.

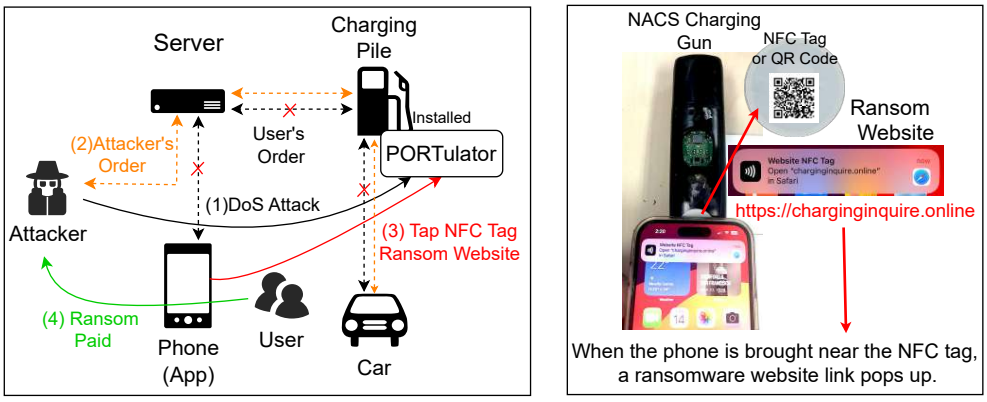
Moreover, the CP line can also be abused similarly. As shown in Figure 7b, injecting a low-duty-cycle PWM signal, such as 5%, can mislead the charging pile into interpreting the session as inactive communication or fault, further halting power delivery. This method offers another vector for reliably disrupting active charging sessions without requiring direct physical interaction.

In real-world public charging environments, repeated interruption of charging sessions can create tangible economic and operational pressure. During peak-demand periods or at high-traffic stations, such disruptions may lead to user complaints, refund requests, scheduling failures, and reputational damage to charging-network operators. In fleet-dependent scenarios, such as taxis, ride-hailing vehicles, logistics vans, or shared mobility systems, even short charging interruptions can propagate into missed service windows and direct financial losses. Therefore, the attack can be realistically leveraged for competitive

sabotage, targeted harassment, or extortion-oriented disruption, making it a practical cyber-physical threat rather than a purely theoretical denial-of-service primitive.

5.2 Case II: Deadlock Attack via CC Port Impedance Manipulation for Ransom

We evaluate a novel ransomware-style attack that exploits CC-line impedance spoofing to force a vehicle into a persistent *deadlock* state: the charging gun becomes mechanically locked and the user cannot terminate or remove the connector. Importantly, this attack requires only brief local access to install a covert device and does *not* rely on Internet connectivity, distinguishing it from conventional ransomware campaigns [9].



(a) Deadlock Attack Applied to Ransom Attack

(b) NFC Triggered Ransom Website Pop-up

Figure 8: Deadlock Attack and NFC-Triggered Ransom Scenario

As illustrated in Figure 8a, the attack unfolds in four stages: (1)**DoS Attack**: The user initiates a legitimate charging session by connecting to a gun embedded with PORTulator. The attacker then remotely triggers a DoS condition (as outlined in § 5.1), halting the process by injecting abnormal signals on the CC or CP line. (2)**Forged Charging Order Replay**: Following disruption, the attacker replays captured CP signals from a previously observed session, initiating a new charging order that appears valid but is under attacker control (see § 5.3). (3)**Ransom Prompt via NFC or QR Code**: When the user returns, the interface is unresponsive and the gun remains locked. An embedded NFC tag or visible QR code on the gun directs the user to a spoofed support page (e.g., `https://charginginquire.online`), which claims that unlocking requires a (cryptocurrency) payment. Devices without NFC support can scan the QR code to reach the same landing page (Figure 8b) (4)**Payment Demand**: The spoofed page instructs the user to pay a ransom to restore operation, effectively converting the compromised charger into an extortion vector.

We successfully demonstrated this attack on a Volkswagen ID.4 using public charging piles operated by TELD and Starcharge in China. The exploit highlights a deeply concerning capability: attackers can gain remote control over EVs' charging states by exploiting infrastructure-side spoofing and interface deadlocks to extract payments from unsuspecting users. This underscores the urgent need for more robust authentication mechanisms, secure session management, and out-of-band validation to prevent such attacks. Detailed information and demo videos can be accessed at `https://github.com/Moriartysherry/ev-charging-station-security`.

5.3 Case III: CAN Bus Signal Injection Attack

We explore how port-adjacent CAN injection could lead to functional compromise of battery management logic when an EV architecture exposes a reachable CAN-domain interface near the charge port.

This class of attack requires two prerequisites: (i) the charging connector (or its harness) must include communication lines that are electrically routed to a CAN-connected charge/port controller (or otherwise bridged to a CAN domain), and (ii) the vehicle must lack strict segmentation/gatewaying or message authentication between the connector-side controller and safety-relevant internal networks. Under these conditions, an inline device can escalate from analog-state manipulation (CC/CP/impedance spoofing) to crafting message-level effects on a reachable CAN segment. In our measurements, such reachability is observed for GB/T 20234.3 (via S+/S–) on specific platforms, whereas our tested CCS/J1772 implementations do not provide any direct connector-side access to an in-vehicle CAN interface, consistent with the negative results reported in Table 2.

R2: clarify platform-specific CAN reachability assumptions.

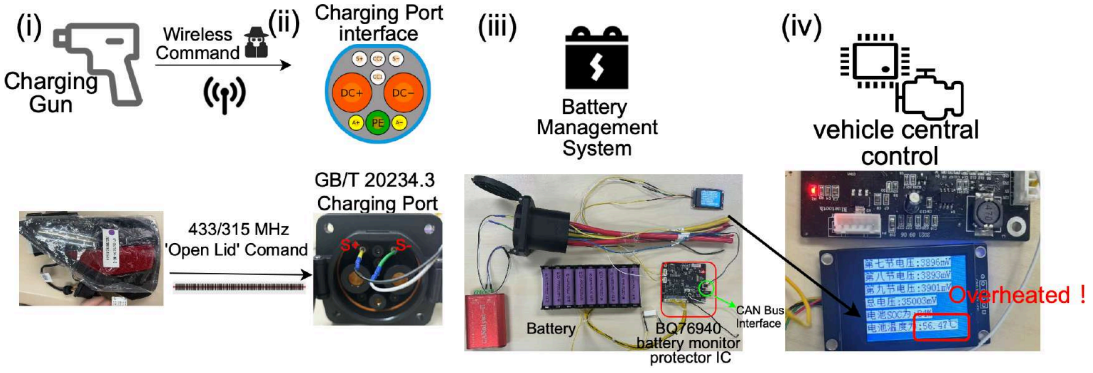


Figure 9: CAN Bus Signal Injection Attack Overview

As shown in Figure 9, the attack begins with the replay of the wireless signal used to open the EV charging port, thereby enabling physical access to the S+/S– communication lines defined in the GB/T 20234.3 standard. These lines are commonly connected to CAN bus-based charging controllers in vehicles such as Denza, BYD, XPeng, and Arcfox.

To simulate a realistic vulnerability, we built a prototype BMS using the TI BQ76940 battery monitor IC and an STM32F103 MCU, both widely adopted in commercial EVs. The BMS is designed to disconnect charging MOSFETs when the battery temperature exceeds 40 $°C$. However, we discovered a stack buffer overflow vulnerability triggered by a specific multi-stage CAN message sequence.

Our proof-of-concept payload bypasses this protection by overwriting control register values, resulting in the MOSFET remaining active even under overheating conditions. In our testbed, this led to continued charging until the battery temperature reached 56.47 $°C$, significantly exceeding the defined thermal threshold. This results in forced charging even under unsafe thermal conditions, with our testbed reaching a battery temperature of 56.47 $°C$ in the red box. This demonstrates a critical safety violation caused by code-level flaws reachable via external CAN access.

Although this experiment is conducted in a simulated environment, its architecture reflects real-world systems. For instance, Tesla's Model S uses a Chargeport ECU that communicates via CAN with internal energy control modules, and lacks strict isolation between the charger-side and internal buses. Our findings suggest that in the absence of proper message authentication or bus isolation, similar injection-based attacks may compromise safety-critical subsystems across various EV platforms. This case study illustrates that CAN bus injection attacks can lead to persistent and dangerous failures, not just momentary service denial, thus exposing a deeper layer of risk within the EV charging ecosystem. Importantly, the practical value of this attack lies not in indiscriminate deployment, but in its ability to escalate charger-side abuse into vehicle-side functional compromise once the architectural preconditions hold. Such an attack is relevant to targeted sabotage against high-value vehicles or fleet operators, coercive disruption, and scenarios where attackers seek to create safety incidents, maintenance burdens, or liability disputes. Therefore, unlike a simple charging interruption, port-adjacent CAN injection provides a realistic path from public charging infrastructure abuse to higher-impact cyber-physical compromise.

R4-3: clarify the practical value of CAN injection.

5.4 Attack Efficacy

Table 2 summarizes the experimental results across seven EV models and six charging standards, validating the practical feasibility of all attacks implemented by PORTulator. The first column denotes the vehicle platform, and the second column lists the charging-port standard/interface tested on that platform (multiple rows per model reflect different ports/regions/configurations). The last column denotes *Potential CAN BUS Injection Attack* on the tested platform (connector-side access to a CAN-domain path), not a universal claim for all implementations of a standard.

R2: platform-specific CAN reachability, not universal to the standard.

Car Models	Charging Ports Standard	DoS Attack	Deadlock Attack	CP PWM Injection Attack	Potential CAN BUS Injection Attack
Tesla Model S	NACS	✔	✔	✔	✔
	SAE J1772	✔	✔	✔	✘
	CCS I	✔	✔	✔	✘
	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✔
Tesla Model 3	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✘
	IEC 62196	✔	✔	✔	✘
	CCS II	✔	✘	✔	✘
Tesla Model Y	NACS	✔	✔	✔	✔
	IEC 62196	✔	✔	✔	✘
	CCS II	✔	✔	✔	✘
Volkswagen ID.4	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✔
ROEWE RX5	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✘
ARCFOX αS	GB/T 20234.2	✔	✔	✔	✘
	GB/T 20234.3	✔	✔	✔	✘
Li Auto L7	IEC 62196	✔	✔	✔	✘
	CCS II	✔	✘	✔	✘

Table 2: Effectiveness of Attacks Across Car Models and Charging Standards. ✔ indicates a successful demonstration; ✘ indicates not observed or not applicable due to hardware/architecture constraints.

DoS and PWM Attacks. Both attacks proved universally effective across all tested configurations. Manipulating CC/CP impedances or injecting low-duty-cycle PWM signals consistently terminated or altered charging sessions, demonstrating cross-standard susceptibility.

Deadlock Attacks. Deadlock success depended on hardware design. Vehicles with electronic locking (e.g., GB/T-based or NACS) experienced full lockout, while CCS II ports lacking lock mechanisms (e.g., Tesla Model 3, Li Auto L7) were unaffected.

CAN Bus Injection. CAN message injection was feasible only on interfaces where the charging connector/harness exposes a vehicle-side communication pair that is electrically routed to a CAN-domain charge/port controller with insufficient isolation. In our tests, this condition was observed on GB/T 20234.3 (via the S+/S– communication lines) and on NACS on specific platforms, where the connector-side controller can be bridged to an in-vehicle CAN segment. In contrast, our tested CCS/J1772 implementations did not provide any connector-side lines that directly map to an in-vehicle CAN interface at the port, and therefore, we did not observe port-adjacent CAN reachability on those configurations. We note that the downstream impact of any injected messages remains architecture-dependent (e.g., segmentation/gatewaying and message authentication), and we detail these assumptions in § 5.3.

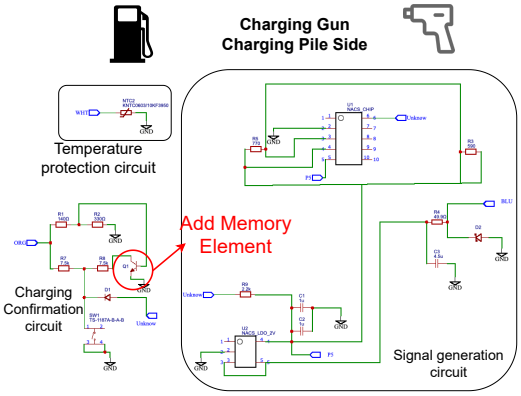
Overall, these results confirm that while DoS-class attacks are universally achievable, advanced exploitation (e.g., deadlock or CAN injection) depends on specific port architectures—highlighting systemic weaknesses across physical and communication layers.

R2, R3-1, R4-3: clarify CAN injection depends on architecture and reachability.

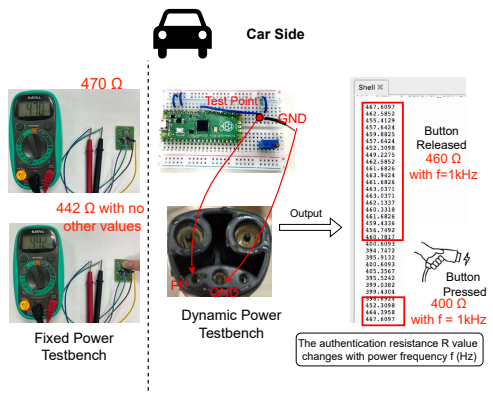
6 Countermeasures

To mitigate vulnerabilities stemming from weak impedance-based authentication in EV charging systems, we propose a twofold countermeasure framework that enhances both signal integrity and spoofing

resistance. Conventional charging authentication relies on a fixed voltage source and resistor-divider network for impedance verification. As illustrated in Figure 3, this static configuration is inherently susceptible to spoofing through resistor emulation.



(a) Solution I – Memory-Integrated Elements (Gun Side)



(b) Solution II – Dynamic Power Source (EV Side)

Solution I: Memory-Integrated Elements. Our first enhancement introduces a *dual-check process* combining legacy fixed-voltage validation with a dynamic signal response test. By integrating memory-capable components—such as transistors and capacitors—into the CC circuit (highlighted in red in Figure 10a), the charging gun gains frequency-dependent impedance characteristics inspired by Tesla's advanced CC design [14–16]. These elements exhibit distinct impedance shifts under variable excitation, making static resistance spoofing infeasible.

Solution II: Dynamic Power Source. On the EV side, we introduce a variable-frequency power source that periodically perturbs the authentication signal. As shown in Figure 10b, the impedance of transistor and capacitor components varies with frequency—$Z_{\text{transistor}} = j2\pi fL$ and $Z_{\text{capacitor}} = 1/(j2\pi fC)$—producing measurable, frequency-dependent responses that are extremely difficult for attackers to replicate. Comparing static and dynamic responses allows rapid identification of abnormal impedance signatures.

To further strengthen validation, we incorporate an optional out-of-band wireless channel (e.g., RF/NFC) for cross-verification and tamper detection. Any deviation between the expected and measured multi-channel responses triggers an alert for manual inspection.

From a deployment perspective, the proposed gun-side augmentation is deliberately low-intrusion and confined to the low-voltage signaling front-end (CC/CP), rather than the high-power conversion path. The added signature elements and the associated sensing/conditioning stage can be realized as a compact inline daughterboard inside the handle/connector enclosure, or integrated onto the existing control PCB near the CC/CP interface, without modifying contactors, power electronics, or thermal design. This makes the mechanism retrofit-friendly: in typical upgrades, only the handle-side electronics module needs replacement while the cable and power stage remain unchanged. To avoid service disruptions for legacy vehicles, the enhanced check is deployed as an additive "second-factor" verification; when the dynamic response is unavailable or inconclusive (e.g., unequipped users, parameter drift), the charger falls back to standard-compliant static validation while logging an alert. In addition, conservative acceptance envelopes and periodic re-baselining can be used to compensate for component tolerances, temperature drift, and aging.

We quantify resilience using detection rate D (higher is better), false positive rate F_p (lower is better), and recovery time T_{rec} (lower is better), and define a composite score:

$$R_s = \alpha D - \beta F_p - \gamma T_{rec},$$

where α, β, and γ reflect operational priorities. To make this metric actionable, we recommend normalizing terms to comparable scales (e.g., D and F_p in $[0, 1]$, and T_{rec} normalized by an operator-defined maximum acceptable recovery time). For interpretability, one can enforce $\alpha + \beta + \gamma = 1$. As an example

[R2, R3-2, R4-3] Add backward-compatibility and safe fallback.

for public charging networks that prioritize both security and user experience, a reasonable default is $\alpha = 0.5$, $\beta = 0.3$, and $\gamma = 0.2$, which favors detection while penalizing false positives more strongly than recovery latency. For high-assurance deployments (e.g., fleet/industrial charging) where safety dominates, a more security-heavy choice such as $\alpha = 0.6$, $\beta = 0.25$, and $\gamma = 0.15$ may be preferred. Conversely, for environments where service continuity is paramount and operator intervention is expensive, increasing β (e.g., $\alpha = 0.4$, $\beta = 0.4$, $\gamma = 0.2$) discourages false positives that could disrupt users.

In our prototype evaluation, we achieve $D = 95\%$, $F_p < 3\%$, and $T_{rec} \approx 0.3\,\text{s}$ under our test conditions, indicating that the proposed dual-check framework can provide strong resilience against transient spoofing and signal tampering while maintaining operational practicality.

[R4-5] Add normalization plus example (α, β, γ) weights and tuning guidance.

7 Related Works

As EVs become increasingly widespread, the security of EVSE has gained critical attention. A growing body of research has investigated vulnerabilities across the charging infrastructure, from remote attacks to physical-layer threats.

Network-based EVSE Vulnerabilities. Prior work has exposed weak backend authentication, misconfigured network endpoints, and Internet-exposed EVSE management systems [8, 17–19]. These studies motivate hardening at the management and network layers; by contrast, our paper focuses on the *front-end* protocol state machine and demonstrates how analog-level signal forgery at the port can bypass both local and network defenses.

Physical Layer EVSE Attacks. Physical-layer threats include broad RF disruption (e.g., Brokenwire [5]) and targeted eavesdropping/credential theft [6]. Relatedly, Dudek et al.'s V2G injector manipulates higher-level V2G exchanges [20]. Our contribution is complementary but distinct: we demonstrate precise *port-level* signal spoofing (impedance/PWM) that forges state transitions without credentials and—critically—we validate these exploits on real vehicles and chargers.

Signal Injection Attacks. Recent work demonstrates unconventional channels for command injection (power-line noise [21] and laser-based audio injection [22, 23]). Inspired by this line, we present the first practical demonstration of low-voltage pilot-line and RF replay attacks targeting charging-port authentication, and we evaluate prototype countermeasures (memory-integrated elements and dynamic-frequency checks).

Practical EVSE Exploitation. Organizations such as SwRI have proposed higher-level defense frameworks and zero-trust approaches [24, 25], and policy work has outlined regulatory needs [26]. Our work fills a technical gap by (i) systematically testing multiple AC/DC standards (GB/T, NACS, CCS, J1772), (ii) demonstrating exploit feasibility on deployed hardware, and (iii) validating concrete hardware/software countermeasures.

8 Discussion

Ethical Considerations. All experiments were performed only on vehicles owned by the authors under controlled conditions. We followed institutional ethical guidelines and confined test signals (PWM pulses, CAN frames, etc.) to hardware-safe ranges to avoid physical damage or data leakage. We consulted safety experts during design and execution to minimise risk.

Responsible Disclosure. We disclosed findings through coordinated channels prior to public release. An initial demo was presented at GEEKCON (selected by the organizers), after which we reported vulnerabilities to the China National Vulnerability Database (NVDB) via the China Automotive Vulnerability Database (CAVD), obtaining five identifiers. Four CVE requests were also submitted through a CNA partner and are under review. Major affected vendors (e.g., Seres, Denza, Zeekr, BYD, XPeng, Arcfox, Dongfeng) were notified.

Limitations & Future Works. PORTulator targets common public chargers and therefore may not generalize to systems employing stronger, dynamic, or crypto-based authentication; we did not evaluate CHAdeMO or ChaoJi connectors. For safety and ethics, we avoided destructive tests, firmware modification, and prolonged backend interactions; BMS safeguards limited some CP-line experiments.

Future work includes broader cross-vendor studies, controlled firmware-level analyses (with vendor cooperation), and evaluating deployment-ready countermeasures such as memory-integrated elements and dynamic-frequency tests.

9 Conclusion

Our research reveals significant vulnerabilities in the authentication mechanisms of EV charging systems, specifically highlighting weak points in widely adopted protocols. Through the use of PORTulator, we successfully demonstrate the feasibility of remote manipulation of charging operations, showcasing attack vectors such as signal injection and manipulation of the CP and CC ports. These vulnerabilities expose public charging infrastructures to potential threats, where attackers could exploit weak authentication processes to disrupt or immobilize vehicles, posing both safety and security risks. Importantly, these vulnerabilities should not be viewed as mere reliability issues or isolated protocol bugs; rather, they provide realistic attack primitives for operational disruption, coercive leverage, and, under architecture-dependent conditions, targeted vehicle-side compromise.

Our findings suggest that current authentication protocols across various charging standards—including GB/T 20234, IEC, SAE J1772, NACS, and CCS—are inadequate in defending against sophisticated spoofing attacks, particularly in systems that rely on static resistance-based authentication mechanisms. The potential for injecting malicious signals, such as CAN bus messages, further underscores the critical need to reevaluate the security of charging infrastructure as EV adoption accelerates globally. In addition to exposing vulnerabilities, we also propose countermeasures to mitigate these risks. These include enhancing authentication protocols by integrating dynamic power, memory electric elements, and multi-layer security checks.

Acknowledgments

We thank the Editor and the anonymous reviewers for their constructive comments and suggestions, which substantially improved the clarity and quality of this manuscript. We also thank the safety experts who provided guidance during the design and execution of the experiments to minimise operational risk. In addition, we acknowledge the coordinated disclosure channels and affected vendors for their responsiveness during the vulnerability reporting process.

Funding

This work was supported by the National Natural Science Foundation of China (NSFC) under Grant No. 62572266.

Conflicts of interest

The authors declare that they have no conflict of interest.

Data availability statement

The experimental data supporting the findings of this study are available from the corresponding author upon reasonable request. The demonstration materials are provided via the project repository https://github.com/Moriartysherry/ev-charging-station-security.

Author contribution statement

Note: Hetian Shi and Shangru Song contributed equally to this work.

Hetian Shi: Conceptualization, Methodology, Hardware and Software Implementation, Investigation, Data Curation, Writing – Original Draft.

Shangru Song: Writing – Original Draft, Investigation, Validation, Data Curation, Formal Analysis.

Yi He: Methodology, Writing – Review & Editing, Validation, Supervision.

Zhenhao Tian: Investigation, Validation, Software, Data Curation, Writing – Original Draft.

Jianwei Zhuge: Supervision, Writing – Review & Editing, Project Administration, Funding Acquisition.

Jian Mao: Supervision, Writing – Review & Editing, Methodology, Project Administration.

Appendices

The table 3 lists four assigned vulnerability IDs affecting major EV vendors, along with brief impact summaries and their corresponding disclosure timelines.

Vuln. ID	Affected Vendor(s)	Impact Summary	Disclosure Timeline
NVDB-CAVD-2025478822	Seres, Denza, Zeekr, BYD, XPeng, Arcfox and Dongfeng Motor	Weak resistance-based authentication allows an attacker to simulate invalid CC states, causing the charger to reject charging (DoS attack).	Reported: 2025-03-18 Acknowledged: 2025-05-22 Fixed: pending
NVDB-CAVD-2025018034	Seres, Denza, Zeekr, BYD, XPeng,Arcfox and Dongfeng Motor	Forged CC resistance locks the charging gun, preventing removal (deadlock attack).	Reported: 2025-03-18 Acknowledged: 2025-05-22 Fixed: pending
NVDB-CAVD-2025864575	Seres, Denza, BYD Arcfox	Malicious CC values trigger discharge mode, draining the EV battery.	Reported: 2025-03-18 Acknowledged: 2025-05-22 Fixed: pending
NVDB-CAVD-2025820938	Denza, BYD, XPeng Arcfox	Bypassing CC2 check enables CAN injection, allowing remote control of charging.	Reported: 2025-03-18 Acknowledged: 2025-04-10 Fixed: pending
NVDB-CAVD-2025633581	Zeekr	Malicious CC values trigger discharge mode, draining the EV battery.	Reported: 2025-05-28 Acknowledged: 2025-06-05 Fixed: pending

Table 3: Vulnerability Disclosure Summary

Authors

Hetian Shi is currently an engineer at Tsinghua University. His research interests include hardware and IoT security, firmware reverse engineering, and physical-layer attacks on cyber-physical systems. His work has appeared in IACR CHES, IEEE S&P, USENIX Security, and TIFS.

Shangru Song is currently a Ph.D. student at the Institute for Network Science and Cyberspace, Tsinghua University. His research interests include IoT security and protocol security.

Yi He is a tenure-track assistant professor at the Institute for Math & AI, Wuhan University. He received his Ph.D. from Tsinghua University in 2024. Before that, he worked as a senior game engineer at NetEase Games. His research interests include the security of hardware, firmware, and protocols in embedded devices, such as drones, satellites, and electric vehicles (EVs).

Zhenhao Tian received his bachelor's degree from Beijing Institute of Technology and is currently pursuing a Master's degree at the Institute for Network Science and Cyberspace, Tsinghua University. His research interests include IoT security and AI for security.

Jianwei Zhuge received his Ph.D. degree from Peking University. He is currently a Research Professor at the Institute for Network Science and Cyberspace, Tsinghua University, and an Adjunct Research Scientist at Zhongguancun Laboratory, Beijing. His work has been published in top-tier venues such as IEEE S&P, ACM CCS, USENIX Security, and NDSS. His research interests include IoT security and AI for security.

Jian Mao (Member, IEEE) received her B.S. and Ph.D. degrees from Xidian University, Xi'an, Shaanxi, China, in 1997 and 2004, respectively. She is a Professor in the School of Cyber Science and Technology, Beihang University, Beijing, China. She is also affiliated with Tianmushan Laboratory, Hangzhou, China, the Hangzhou Innovation Institute, Beihang University, Hangzhou, China, and Zhongguancun Laboratory, Beijing, China. Her research interests include IoT security, web security, and mobile security.

References

[1] K. Iehira, H. Inoue, and K. Ishida, "Spoofing attack using bus-off attacks against a specific ecu of the can bus," in *2018 15th IEEE annual consumer communications & networking conference (CCNC)*. IEEE, 2018, pp. 1–4.

[2] M. Conti, D. Donadel, R. Poovendran, and F. Turrin, "Evexchange: A relay attack on electric vehicle charging system," in *European Symposium on Research in Computer Security*. Springer, 2022, pp. 488–508.

[3] A. Kailus, D. Kern, and C. Krauß, "Self-sovereign identity for electric vehicle charging," in *International Conference on Applied Cryptography and Network Security*. Springer, 2024, pp. 137–162.

[4] A. Venčkauskas, M. Taparauskas, Š. Grigaliūnas, and R. Brūzgienė, "Enhancing communication security an in-vehicle wireless sensor network," *Electronics*, vol. 13, no. 6, p. 1003, 2024.

[5] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of ccs electric vehicle charging," in *Proceedings of the 30th Annual Network and Distributed System Security Symposium (NDSS 2023)*, San Diego, California, USA, Mar. 2023.

[6] R. Baker and I. Martinovic, "Losing the car keys: Wireless {PHY-Layer} insecurity in {EV} charging," in *28th USENIX Security Symposium (USENIX Security 19)*, 2019, pp. 407–424.

[7] T. Nasr, S. Torabi, E. Bou-Harb, C. Fachkha, and C. Assi, "Chargeprint: A framework for internet-scale discovery and security analysis of ev charging management systems." in *NDSS*, 2023.

[8] G. Vailoces, A. Keith, A. Almehmadi, and K. El-Khatib, "Securing the electric vehicle charging infrastructure: An in-depth analysis of vulnerabilities and countermeasures," in *Proceedings of the Int'l ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, 2023, pp. 31–38.

[9] Anonymous, "Demo: Ransom Vehicle through Charging Pile," in *Proceedings of the 2023 Inaugural Symposium on Vehicle Security and Privacy*, ser. VehicleSec '23, 2023.
[10] "Definition and implementation of a global ev park charge," accessed: 2023-10-05. [Online]. Available: https://www.yumpu.com/en/document/read/39489467/definition-and-implementation-of-a-global-ev-park-charge
[11] "Physical connection of dc charging process," accessed: 2023-10-05. [Online]. Available: https://wattsaving.com/blogs/knowledge-base/physical-connection-of-dc-charging-process
[12] W. contributors. Combined charging system. [Online]. Available: https://en.wikipedia.org/wiki/Combined_Charging_System
[13] Wikipedia contributors, "Sae j1772 — Wikipedia, the free encyclopedia," 2024, [Online; accessed 18-April-2024]. [Online]. Available: https://en.wikipedia.org/wiki/SAE_J1772
[14] Tesla, Inc., "North american charging standard: Technical specification (ts-0023666)," 2022, accessed: 2026-01-16. [Online]. Available: https://digitalassets.tesla.com/tesla-contents/image/upload/North-American-Charging-Standard-Technical-Specification-TS-0023666
[15] SAE International, "J3400: North american charging system (nacs) for electric vehicles," 2023, accessed: 2026-01-16. [Online]. Available: https://www.sae.org/standards/j3400-north-american-charging-system-nacs-electric-vehicles
[16] "Communication on a pilot wire," Patent US20 120 002 714A1, 2012, accessed: 2026-01-16. [Online]. Available: https://patents.google.com/patent/US20120002714A1/en
[17] R. Varriale, R. Crawford, and M. Jaynes, "Risks of electric vehicle supply equipment integration within building energy management system environments: A look at remote attack surface and implications," in *National Cyber Summit (NCS) Research Track 2021*. Springer, 2022, pp. 163–173.
[18] C. Hille and M. Allhoff, "Ev charging: Mapping out the cyber security threats and solutions for grids and charging infrastructure," *UtiliNet Europe*, 2018.
[19] J. Johnson, B. Anderson, B. Wright, J. Quiroz, T. Berg, R. Graves, J. Daley, K. Phan, M. Kunz, R. Pratt *et al.*, "Cybersecurity for electric vehicle charging infrastructure," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2022.
[20] S. Dudek, J.-C. Delaunay, and V. Fargues, "V2g injector: Whispering to cars and charging units through the power-line," in *Proceedings of the SSTIC (Symposium sur la sécurité des technologies de l'information et des communications), Rennes, France*, 2019, pp. 5–7.
[21] Y. Wang, H. Guo, and Q. Yan, "Ghosttalk: Interactive attack on smartphone voice system through power line," in *Proceedings of the Network and Distributed System Security (NDSS) Symposium 2022*. San Diego, CA, USA: Internet Society, Apr. 2022.
[22] H. Shi, Y. He, Q. Wang, J. Zhuge, Q. Li, and X. Liu, "Laser-based command injection attacks on voice-controlled microphone arrays," *IACR Transactions on Cryptographic Hardware and Embedded Systems (CHES)*, vol. 2024, no. 2, pp. 654–676, 2024.
[23] T. Sugawara, B. Cyr, S. Rampazzi, D. Genkin, and K. Fu, "Light commands:{Laser-Based} audio injection attacks on {Voice-Controllable} systems," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 2631–2648.
[24] S. R. Institute, "Electric vehicle charging cybersecurity vulnerabilities," https://www.swri.org/press-release/electric-vehicle-charging-cybersecurity-vulnerabilities, 2024, accessed: 2024-07-25.
[25] ——, "Electric vehicle cybersecurity services," https://www.swri.org/industry/automotive-software-electronics/electric-vehicle-cybersecurity-services, 2024, accessed: 2024-07-25.
[26] S. A. Wasumwa, "Safeguarding the future: A comprehensive analysis of security measures for smart grids," *World Journal of Advanced Research and Reviews*, vol. 19, no. 1, pp. 847–871, 2023.