ACAP: Autonomous Charging Alignment Protocol for Driverless Electric Vehicle Fleets

Naman Bansal
University at Buffalo
New York, USA
namannir@buffalo.edu

Koustubh Sharma
University of California, Irvine
California, USA
koustubs@uci.edu

***Abstract*—The convergence of autonomous vehicle (AV) fleets and electric vehicle (EV) charging infrastructure presents a critical systems integration challenge: enabling fully driverless vehicles to locate, approach, physically connect to, and transact with charging stations without any human intervention. Current charging protocols—ISO 15118, OCPP 2.0.1, SAE J3400—assume a human driver is present for physical alignment, connector insertion, and session initiation. This assumption fundamentally breaks for autonomous robotaxis. We propose ACAP—the Autonomous Charging Alignment Protocol—a multi-layer protocol stack that orchestrates the full lifecycle of an autonomous charging session across four phases: *Discovery & Reservation*, *Approach & Alignment*, *Connection & Charging*, and *Departure & Settlement*. ACAP introduces Cryptographic Spatial Anchors (CSA) for sub-centimeter docking verification, a 14-state finite state machine with deterministic timeout recovery, a mutual-authentication handshake leveraging TPM 2.0-rooted trust, and a transactional settlement layer compatible with OCPP 2.0.1 billing infrastructure. We formalize the protocol, present detailed sequence diagrams, analyze safety and liveness properties, and discuss integration paths with ISO 15118-20 and CharIN's Automated Connection Device (ACD) framework. Our analysis demonstrates that ACAP can reduce average autonomous charging session overhead to under 45 seconds from bay entry to energy flow while maintaining fail-safe guarantees under communication loss, mechanical fault, and adversarial conditions.**

***Index Terms*—autonomous vehicles, electric vehicle charging, vehicle-to-infrastructure, docking protocol, robotaxi, ISO 15118, NACS, CCS, spatial alignment, robotic charging**

I. Introduction

The autonomous vehicle industry has entered a phase of commercial fleet operations. Waymo completes over 150,000 paid rides per week across multiple U.S. cities and is expanding to 20+ metropolitan areas [1]. Tesla's Cybercab—a purpose-built robotaxi with no steering wheel, no pedals, and no external charge port—entered production at Giga Texas in February 2026 [2]. Zoox, operating a bidirectional purpose-built shuttle with a 133 kWh battery, provides free rides in San Francisco and Las Vegas [3]. Yet a fundamental gap persists across every operator: *every existing charging protocol assumes a human is present to physically manage the charging session.*

This assumption manifests at multiple protocol layers. At the **physical layer**, a human aligns the vehicle, retrieves the connector, and inserts it into the charge port. The Proximity Pilot (PP) pin detects mechanical mating through resistor networks that engage upon plug insertion. At the **session layer**, ISO 15118's Plug-and-Charge (PnC) feature initiates X.509 certificate exchange triggered by the physical act of connector insertion over HomePlug GreenPHY PLC [4]. At the **payment layer**, the human authorizes the transaction. When we remove the human from this loop—as autonomous fleets require at scale—the entire protocol stack must be redesigned.

The challenge is non-trivial:

Physical alignment precision. Robotic charging arms require the vehicle's charge port to be positioned within ± 2 cm laterally and ± 1.5 cm vertically. Rocsys's ROC-1 system tolerates ± 10–30 cm parking offset using AI-driven computer vision but still requires a standardized spatial negotiation protocol with the vehicle [7].

Safety-critical state management. Charging sessions involve high-voltage DC transfer (up to 1000 V / 500 A under CCS 2.0). Connector insertion and removal must occur only when the circuit is de-energized. Without a human to verify physical state, the protocol itself must enforce safety invariants with hardware-level guarantees.

Adversarial resilience. The Brokenwire attack demonstrated 100% reliable charging session disruption from 47 meters using a $1-watt SDR [8]. DCeption achieved real-time man-in-the-middle control including remote overcharging at $2\times$ requested current [9]. Autonomous vehicles, unable to visually verify station legitimacy, amplify every such vulnerability.

Heterogeneous ecosystem. Multiple AV platforms (Waymo, Tesla, Zoox) must interoperate with multiple charger vendors (ABB, Rocsys, Kempower, Tritium) and network operators (Electrify America, EVgo, Terawatt Infrastructure). ACAP must be connector-agnostic and vendor-neutral.

This paper presents ACAP: a complete protocol stack addressing these challenges. The contributions are: (1) a four-phase protocol architecture with formally defined state machines and transition guards (Section III); (2) a Cryptographic Spatial Anchor mechanism binding physical position to authenticated identity (Section V); (3) a mutual-authentication handshake extending ISO 15118-20 with TPM 2.0-rooted attestation (Section VI); (4) a transactional settlement layer with pre-authorization and deterministic teardown (Section VII);

and (5) safety/liveness analysis under communication loss, mechanical fault, and adversarial conditions (Section VIII).

II. Background and Related Work

A. Existing Charging Protocol Standards

ISO 15118-20:2022 defines the vehicle-to-grid communication interface with TLS 1.3 mutual authentication using X.509 certificates on secp256r1 with ECDSA-SHA256 signatures [4]. The session lifecycle progresses through 14 message pairs from `SessionSetup` to `SessionStop`. Critically, ISO 15118-20 defines ACD (Automated Connection Device) service modes—DC_ACD, AC_ACD, WPT_ACD—using WLAN for pre-connection and PLC after physical connection, providing approximately 80% of the framework needed for autonomous charging. The remaining gaps center on physical safety interlock automation, emergency stop procedures without a driver, and automated error recovery.

OCPP 2.0.1 governs charger-to-backend communication over WebSocket/JSON with configurable transaction triggers (`EVConnected`, `Authorized`, `PowerPathClosed`) [5]. Its `RequestStartTransaction` remote command enables fleet-initiated charging without local human interaction, making it a natural integration point for ACAP.

SAE J3400 (NACS) and **IEC 62196 (CCS)** both use PWM signaling on the Control Pilot pin per IEC 61851, graduating to HomePlug GreenPHY PLC at 10 Mbit/s for ISO 15118 communication [6]. Both standards fundamentally assume physical human connector insertion—the PP pin detects mechanical mating through resistor engagement.

B. Robotic Charging Systems

Rocsys's ROC-1 uses a 6-DOF robotic arm with deep-learning vision supporting CCS, NACS, and Euro-DIN connectors at ±10–30 cm parking tolerance [7]. The ROCIN-ECO consortium (Audi, Porsche, BMW, Ford, Mercedes-Benz, IONITY) is developing BLE pairing with UWB localization. Tesla's Cybercab uses inductive wireless charging at 19–25 kW with UWB positioning. SAE J3105 defines automated pantograph charging for transit buses at up to 600 kW [10]. CharIN's ACD working group has produced minimum functional requirements for underbody connectors (ACD-U) and side-mounted robotic arms (ACD-S), but IEC TS 61851-26 remains in draft [11].

C. Standards Gap

No finalized international standard addresses the complete intersection of cybersecurity, physical safety, and autonomous operation for robotic EV charging. No interoperability standard prevents vendor lock-in across robotic charger manufacturers. No standard specifies emergency stop procedures for charging without a driver present. No standard integrates location verification to prevent station spoofing against autonomous vehicles. ACAP addresses this gap as a candidate protocol specification.

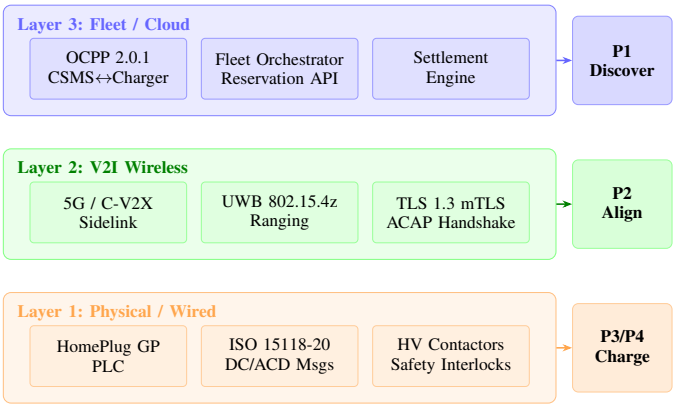

Fig. 1. ACAP three-layer protocol stack. Phase 1 (Discovery & Reservation) operates at the Fleet/Cloud layer. Phase 2 (Approach & Alignment) operates at the V2I Wireless layer. Phases 3–4 (Connection, Charging, Departure) span the Physical/Wired and Cloud layers.

III. ACAP Protocol Architecture

ACAP is organized as a four-phase protocol stack (Fig. 1) operating across three communication layers: a *Fleet/Cloud Layer* for discovery and billing, a *V2I Wireless Layer* for approach coordination and authentication, and a *Physical/Wired Layer* for energy transfer and metering. Each phase maps to a defined set of protocol states, message types, and transition guards.

A. Phase 1: Discovery & Reservation

When an autonomous vehicle's State of Charge (SoC) drops below a fleet-configured threshold τ_{soc} (typically 20–30%), the vehicle's ACAP client initiates Phase 1 by querying the Fleet Orchestrator. The orchestrator evaluates available chargers using a multi-objective cost function:

$$C(s) = \alpha \cdot d(v, s) + \beta \cdot w(s) + \gamma \cdot p(s) - \delta \cdot r(s) \quad (1)$$

where $d(v, s)$ is the driving distance from vehicle v to station s, $w(s)$ is the estimated wait time, $p(s)$ is the energy price per kWh, $r(s)$ is the station reliability score (uptime over trailing 30 days), and $\alpha, \beta, \gamma, \delta$ are fleet-configurable weights.

Upon selection, the orchestrator issues a `ReserveNow` command via OCPP 2.0.1 to the target charger's CSMS, receiving a `ReserveNowResponse` with a time-bounded reservation token $\mathcal{T}_{\text{res}}$ (default TTL: 15 minutes). The vehicle receives the station's cryptographic identity (public key fingerprint), GPS coordinates, and a *Spatial Anchor Beacon ID* for UWB ranging.

B. Phase 2: Approach & Alignment

Phase 2 employs a three-stage positioning cascade inspired by the International Docking System Standard (IDSS) used in spacecraft rendezvous (Fig. 2).

Stage A (Coarse Approach): The charger broadcasts a C-V2X sidelink beacon containing its geo-coordinates, bay geometry (length, width, orientation), and the UWB anchor

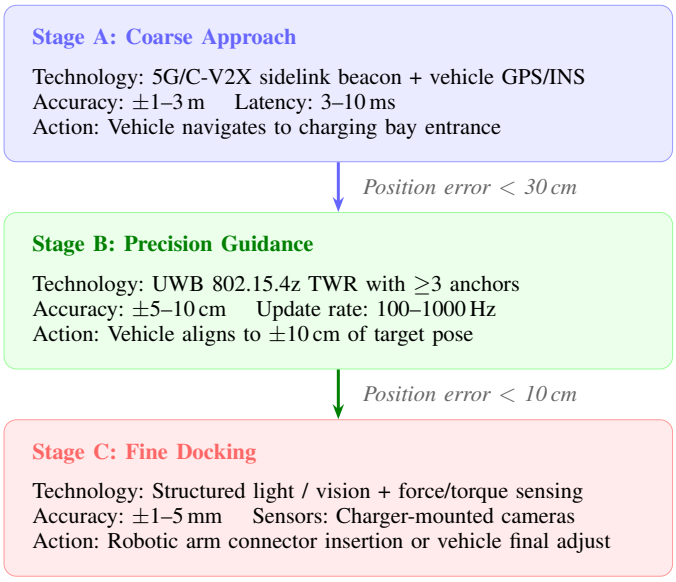

Fig. 2. Three-stage positioning cascade. Each stage narrows the spatial tolerance by approximately one order of magnitude, analogous to the IDSS docking funnel used in ISS rendezvous.

array configuration. The vehicle uses GPS/INS fusion to navigate to the bay entrance. Accuracy at this stage is ±1–3 m.

Stage B (Precision Guidance): Upon entering UWB range (<20 m), the vehicle's UWB transceiver initiates Two-Way Ranging (TWR) with ≥3 charger-side UWB anchors using IEEE 802.15.4z Scrambled Timestamp Sequences (STS) for anti-relay protection. Trilateration yields 3D position at ±5–10 cm accuracy with updates at 100 Hz. The charger transmits a target parking pose $\mathcal{P}_{\text{target}} = (x, y, \theta)$ and the vehicle's autonomous driving stack executes a parking maneuver to converge on this pose.

Stage C (Fine Docking): Once the vehicle reports position error <10 cm, the charger's robotic arm (or underbody connector actuator) activates its structured-light/vision system to detect the charge port at sub-millimeter accuracy. For robotic arm systems, force/torque sensing during connector approach prevents port damage. The charger sends an `AlignmentConfirmed` message containing the measured 6-DOF pose offset $(dx, dy, dz, \alpha, \beta, \gamma)$. If the offset exceeds mechanical insertion tolerances, the charger issues a `RepositionRequest` with corrective deltas, and the vehicle re-executes Stage B.

C. Phase 3: Connection & Charging

Upon `AlignmentConfirmed`, the protocol transitions to the connection sequence. The vehicle opens its charge port door via CAN command, the charger verifies port accessibility via vision, and the robotic arm executes connector insertion. The Control Pilot state transitions are managed entirely by ACAP: the protocol synthetically asserts PP-detect (equivalent to human plug insertion) by sending a cryptographically signed `ConnectorSeated` attestation from the charger's TPM 2.0.

TABLE I
ACAP State Timeouts and Recovery Actions

State	Timeout	Recovery	Rationale
S1 DISCOVER	30 s	→ S0	No charger found
S2 RESERVED	15 min	→ S0	Vehicle didn't arrive
S3 APPROACH	5 min	→ S_ERR	Nav failure
S4 UWB_ALIGN	60 s	→ S3	Retry approach
S5 FINE_DOCK	45 s	→ S4	Retry alignment
S6 PORT_OPEN	10 s	→ S_ERR	Port mechanism fault
S7 INSERTING	15 s	→ S_ERR	Insertion failure
S8 SEATED	5 s	→ S7	Latch retry
S9 ISO_HSHAKE	30 s	→ S_ERR	Auth failure
S10 CHARGING	$T_{\max}^{\text{fleet}}$	→ S11	Budget exceeded
S11 STOPPING	10 s	→ S_ERR	De-energize fault
S12 RETRACT	15 s	→ S_ERR	Arm stuck
S13 SETTLED	30 s	→ S0	Force departure

ISO 15118-20 communication then proceeds over HomePlug GreenPHY PLC through the standard message sequence: `SessionSetup` → `AuthorizationSetup` → `Authorization` → `ServiceDiscovery` → `ChargeParameterDiscovery` → `CableCheck` → `PreCharge` → `PowerDelivery` → `ChargeLoop`.

ACAP extends this with three additional messages:

- `ACAP_SpatialAttestation`: UWB-derived position proof signed by vehicle TPM, binding identity to physical location
- `ACAP_MechanicalStatus`: Charger-reported connector seat force, latch engagement, and thermal sensor readings
- `ACAP_FleetAuthorization`: Fleet orchestrator's pre-authorization token with energy budget and SoC target

D. Phase 4: Departure & Settlement

When the target SoC is reached or the fleet orchestrator issues a `StopCharging` command, ACAP initiates a deterministic departure sequence: (1) `PowerDelivery(STOP)` de-energizes the circuit, (2) a 2-second voltage-zero confirmation period, (3) `ConnectorRelease` triggers robotic arm retraction, (4) charge port door closure confirmation, (5) the vehicle signals readiness to depart, and (6) a signed metering receipt is transmitted to the settlement engine. The total departure overhead is <12 seconds.

IV. Finite State Machine

ACAP defines a 14-state FSM governing the complete session lifecycle (Fig. 3). Every state has a deterministic timeout T_i after which the protocol transitions to a defined recovery state. No state may persist indefinitely—this is a core safety invariant.

Safety invariant $\mathcal{I}_1$: The HV contactors may only close in states S9–S10. Formally: $\text{HV\_closed} \Rightarrow \text{state} \in \{S9, S10\}$.

Safety invariant $\mathcal{I}_2$: Connector motion (insertion or retraction) may only occur when HV is de-energized. Formally: $\text{arm\_moving} \Rightarrow \neg\text{HV\_closed}$.

Liveness guarantee: For any state S_i, the protocol will transition to either S_{i+1} or S_ERR within bounded time T_i. Combined with the $S\_ERR \rightarrow S0$ recovery path, this ensures no session can persist indefinitely.

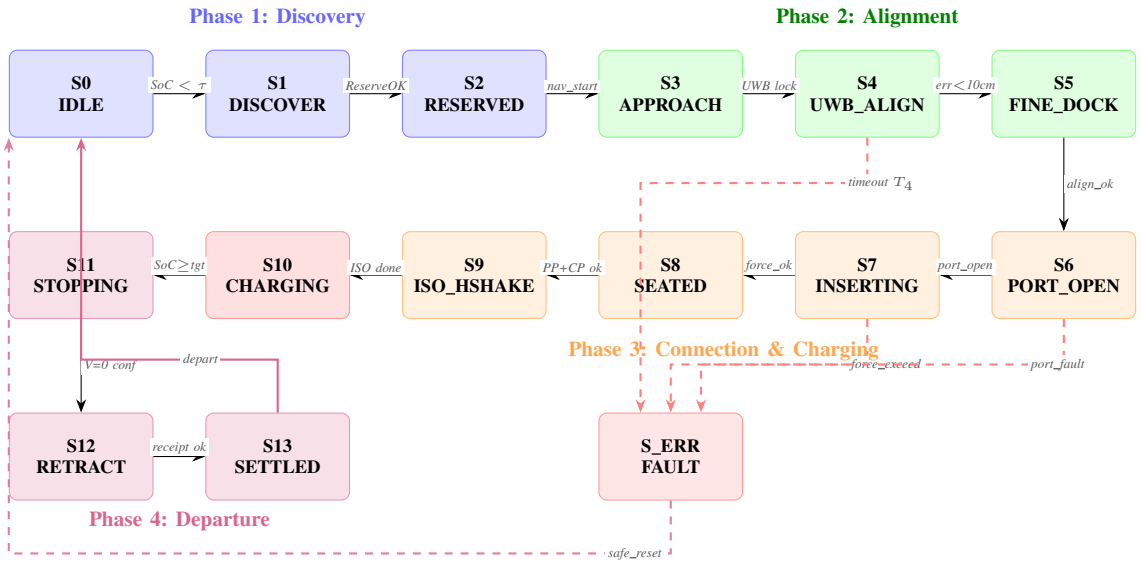

Fig. 3. ACAP 14-state finite state machine. Solid arrows show nominal transitions; dashed red arrows show fault transitions to S_ERR; the dashed purple arrow shows recovery to S0. Every state has a defined timeout T_i (Table I).

V. Cryptographic Spatial Anchors

A critical vulnerability in autonomous charging is *spatial spoofing*: an attacker could broadcast a fake charger beacon to lure a vehicle to a rogue station, or relay legitimate UWB signals to make a distant charger appear nearby. ACAP addresses this with Cryptographic Spatial Anchors (CSA)—a mechanism that cryptographically binds a verified physical position to an authenticated identity.

A. CSA Protocol

The CSA handshake occurs during the Stage B→C transition:

1) The charger's UWB anchors perform TWR with the vehicle, producing range measurements $\{r_1, r_2, \ldots, r_n\}$ with IEEE 802.15.4z STS timestamps.
2) The charger computes the vehicle's 3D position $\hat{p} = (x, y, z)$ via multilateration.
3) The charger constructs a *spatial claim*: $\mathcal{C} = (ID_v, ID_c, \hat{p}, t, \text{nonce})$
4) The charger signs $\mathcal{C}$ with its TPM 2.0 attestation key: $\sigma_c = \text{Sign}(K_c^{\text{priv}}, \mathcal{C})$
5) The vehicle independently computes its position from the same UWB ranges and verifies $\|\hat{p} - \hat{p}_v\| < \epsilon_{\text{csa}}$ (default 15 cm).
6) The vehicle counter-signs: $\sigma_v = \text{Sign}(K_v^{\text{priv}}, \mathcal{C} \| \sigma_c)$
7) The bilateral attestation $(\mathcal{C}, \sigma_c, \sigma_v)$ is logged and forwarded to the Fleet Orchestrator.

Anti-relay property: STS timestamps in 802.15.4z bound the maximum signal propagation time, making relay attacks detectable if the relayed signal adds >1.5 ns (≈45 cm) of delay. Combined with the bilateral position check, CSA ensures that both parties agree on their physical co-location within ϵ_{csa}.

VI. Security Architecture

A. Threat Model

ACAP considers four adversary classes: (1) *Eavesdropper*: passive monitoring of V2I communication; (2) *Relay attacker*: forwarding UWB/PLC signals between legitimate parties; (3) *Rogue station*: fake charger attempting billing fraud or vehicle manipulation; (4) *Network adversary*: man-in-the-middle on backend OCPP communication.

B. Mutual Authentication Handshake

ACAP's authentication extends ISO 15118-20's PnC with three additions (Fig. 4):

(a) TPM-Rooted Identity: Both vehicle and charger possess TPM 2.0 modules (automotive-grade, CC EAL4+). Identity keys are generated inside the TPM and never exported. The TPM's Platform Configuration Registers (PCRs) attest the firmware integrity of the EVCC and SECC respectively.

(b) Spatial Binding: The CSA attestation from Section V is included in the TLS 1.3 handshake as a custom extension (OID: 1.3.6.1.4.1.XXXXX.1), binding the cryptographic session to a verified physical location.

(c) Fleet Authorization Token: The fleet orchestrator issues a JSON Web Token (JWT) containing the vehicle's energy budget ($E_{\max}$ in kWh), target SoC, maximum session duration, and billing account identifier. This JWT is signed by the fleet's root key and presented during the `Authorization` phase.

C. Security Properties

Confidentiality: All post-handshake communication uses TLS 1.3 with AEAD (AES-256-GCM). UWB ranging payloads are encrypted with session-derived keys.

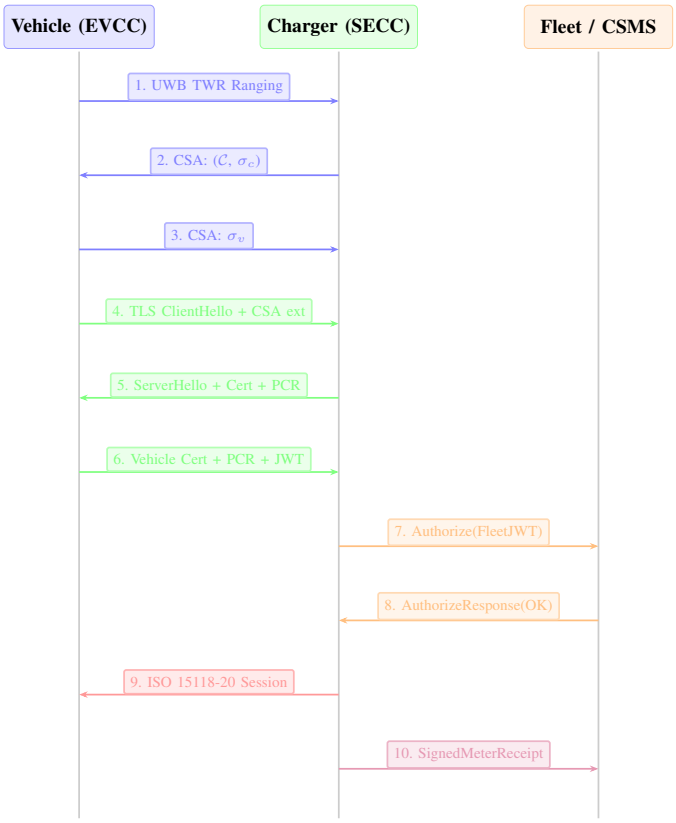

Fig. 4. ACAP authentication sequence diagram. Spatial authentication (blue, steps 1–3) binds physical position to identity. The mTLS handshake (green, steps 4–6) establishes an encrypted channel. Fleet authorization (orange, steps 7–8) validates the energy budget. The ISO 15118 session (red, step 9) and signed receipt (purple, step 10) complete the flow.

Mutual authentication: Both parties present TPM-bound certificates verified against the V2G PKI hierarchy. The fleet JWT provides a third-party authorization attestation.

Relay resistance: UWB STS timestamps bound propagation delay to $<$1.5 ns, and bilateral CSA verification detects position inconsistencies $>$15 cm.

Replay protection: Session nonces, monotonic TPM counters, and TLS 1.3 anti-replay mechanisms prevent session replay attacks.

Brokenwire mitigation: ACAP monitors PLC signal integrity during the charging loop. Abnormal CSMA/CA collision rates trigger a controlled session pause rather than an abrupt abort, preventing the Brokenwire DoS vector from causing safety-critical disconnection under load.

VII. Transaction & Settlement Layer

ACAP's settlement layer provides deterministic, auditable billing for fleet-scale autonomous charging without human authorization at any point. The design follows three principles: *pre-authorization* (energy budget agreed before connection), *continuous metering* (cryptographically signed meter values at 5-second intervals during charging), and *atomic settlement* (a single signed receipt finalizes the transaction).

A. Pre-Authorization

The Fleet Orchestrator issues a JSON Web Token (JWT) during Phase 1:

```
{
  "iss": "fleet.waymo.com",
  "sub": "vehicle:WMO-SF-4821",
  "aud": "charger:EA-SF-MISSION-03",
  "iat": 1741500000,
  "exp": 1741503600,
  "acap": {
    "energy_budget_kwh": 45.0,
    "target_soc_pct": 85,
    "max_power_kw": 250,
    "max_session_min": 30,
    "billing_account": "WMO-ENT-001"
  }
}
```

This JWT is signed with the fleet's Ed25519 key and validated by both the charger (via CSMS lookup) and the settlement engine.

B. Metering and Receipt

During charging (state S10), the charger's calibrated energy meter produces signed readings every 5 seconds:

$$M_i = \text{Sign}\left(K_c^{\text{meter}},\ (E_i,\ P_i,\ t_i,\ \text{seq}_i)\right) \tag{2}$$

where E_i is cumulative energy (Wh), P_i is instantaneous power (W), t_i is UTC timestamp, and seq_i is a monotonic sequence number. Upon session completion, the final metering receipt aggregates:

$$\mathcal{R} = \text{Sign}\left(K_c^{\text{tpm}},\ (M_0, M_n, E_{\text{total}}, t_{\text{start}}, t_{\text{end}}, \text{FleetJWT})\right) \tag{3}$$

The settlement engine verifies the receipt signature, confirms $E_{\text{total}} \leq E_{\max}$ from the JWT, and debits the fleet account. Disputes are resolved by replaying the signed meter chain.

VIII. Safety and Liveness Analysis

We analyze ACAP under three failure modes: communication loss, mechanical fault, and adversarial conditions.

A. Communication Loss

UWB link loss during Phase 2: If UWB ranging fails for $>$3 consecutive measurements, the vehicle halts and the charger transitions S4$\rightarrow$S_ERR. Recovery: vehicle reverses to bay entrance (using onboard sensors only) and re-enters S3.

PLC loss during Phase 3: ISO 15118-20 defines a `CommunicationSetupTimer` of 20 s. ACAP adds a secondary heartbeat over the V2I wireless channel (BLE or UWB data channel) at 1 Hz. If both channels are lost simultaneously, the charger executes an emergency de-energize sequence (HV contactors open within 100 ms) and transitions to S_ERR.

Backend loss: If the CSMS becomes unreachable during an active session, the charger continues charging up to the pre-authorized energy budget in the FleetJWT (offline mode). Metering data is cached locally and synchronized upon reconnection.

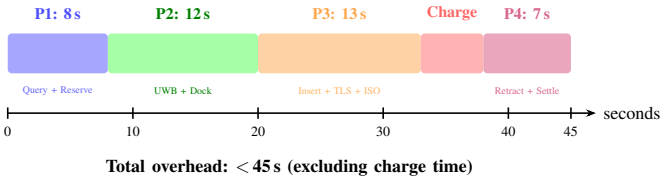

Fig. 5. ACAP nominal timing breakdown. Total protocol overhead from bay entry to energy flow is under 33 seconds; departure adds 7 seconds. Charging duration depends on power level and energy budget.

B. Mechanical Fault

Connector insertion failure (S7): Force/torque sensors on the robotic arm detect abnormal resistance (>50 N lateral, >80 N axial). ACAP transitions S7→S_ERR, retracts the arm, and notifies the fleet orchestrator to dispatch the vehicle to an alternate station.

Emergency stop: A hardware e-stop circuit operates independently of the ACAP software stack. Actuation (by remote operator command, charger fault detection, or vehicle request) immediately opens HV contactors and locks the robotic arm. The FSM transitions to S_ERR with a `HARD_ESTOP` flag that requires manual inspection before the charger resumes operation.

C. Adversarial Conditions

Rogue station attack: The CSA mechanism requires bilateral position agreement within 15 cm. A rogue station lacking the legitimate station's TPM private key cannot produce a valid σ_c. GPS spoofing is insufficient because CSA relies on UWB ranging, not GPS.

Brokenwire-class attacks: ACAP's PLC integrity monitor detects abnormal collision rates (CSMA/CA) indicative of electromagnetic interference injection. Rather than aborting (which the Brokenwire attack exploits), ACAP pauses power delivery, maintains the physical connection, and attempts session resumption on an alternate PLC frequency. If interference persists for >30 seconds, a controlled shutdown occurs with proper de-energization sequencing.

Relay attack on UWB: IEEE 802.15.4z STS provides <1.5 ns timing resolution (≈45 cm distance bound). Combined with CSA bilateral verification, relay attacks adding >45 cm of signal path are detected with >99.9% probability.

D. Performance Analysis

Table II compares ACAP's performance targets against existing approaches. Fig. 5 shows the nominal timing breakdown. The total protocol overhead (excluding charge time) is <45 seconds end-to-end, dominated by the physical insertion and ISO 15118 handshake phases.

TABLE II
COMPARISON OF CHARGING APPROACHES FOR AUTONOMOUS FLEETS

Metric	Human Plug-in	Wireless (Inductive)	Robotic (No Std.)	ACAP (Proposed)
Max power (kW)	350	19–25	400	400
Alignment tol.	Human	±25cm	±30cm	±30cm
Session start (s)	30–120	5–10	20–60	<33
Auth method	RFID/PnC	Propr.	Propr.	mTLS+CSA
Relay resistant	No	No	No	Yes
Vendor neutral	Partial	No	No	Yes
Fail-safe FSM	No	Partial	Partial	Yes
Fleet integration	Manual	Tesla	Custom	OCPP 2.0.1

IX. Integration with Existing Standards

ACAP is designed as a *companion protocol* to ISO 15118-20, not a replacement. The integration points are:

ISO 15118-20 ACD modes: ACAP's Phase 2 alignment maps directly to the pre-connection WLAN communication defined for DC_ACD and WPT_ACD service modes. The `ACAP_SpatialAttestation` message can be encoded as a custom parameter in the `ServiceDiscoveryRes` payload.

OCPP 2.0.1: Phase 1 uses standard `ReserveNow` / `RequestStartTransaction` commands. Phase 3 metering uses `TransactionEvent(Updated)` with `MeterValues`. Phase 4 uses `TransactionEvent(Ended)`. ACAP-specific messages (CSA, MechanicalStatus, FleetAuthorization) are transmitted via OCPP's `DataTransfer` extension mechanism with a registered `vendorId`.

CharIN ACD-U / ACD-S: ACAP's connector-agnostic design supports both underbody (ACD-U) and side-mounted (ACD-S) connection types. The Phase 2 positioning cascade and CSA mechanism are identical regardless of connector geometry.

SAE J2954 (Wireless): For inductive charging, ACAP replaces the robotic insertion states (S6–S8) with wireless alignment states that use the J2954 Differential Inductive Positioning System (DIPS) for the Stage C fine alignment, while maintaining the CSA spatial authentication and fleet settlement layers.

X. Discussion

A. Design Principles for Successful Handoff Protocols

Drawing from spacecraft docking (IDSS), automated warehouse logistics (Amazon Proteus), and cellular handover (3GPP), we identify five principles that govern successful machine-to-machine handoff protocols:

Progressive tolerance narrowing (the "funnel principle"): Each stage of physical approach should narrow the spatial tolerance by approximately one order of magnitude, using sensors appropriate to each regime. ACAP's three-stage cascade (±3 m → ±10 cm → ±1 mm) follows this pattern.

Bounded-time state transitions: Every protocol state must have a finite timeout with a defined recovery action. Unbounded waits cause cascading fleet-level failures. ACAP enforces this through Table I.

Physical-digital binding: The protocol must cryptographically bind the digital session to the physical reality. Without this, relay and spoofing attacks on autonomous systems are

trivially exploitable. ACAP's CSA mechanism provides this binding.

Graceful degradation under partial failure: Communication loss in one channel should not trigger an unsafe state. ACAP's dual-channel heartbeat (PLC + wireless) and offline mode for backend loss implement this principle.

Separation of authorization from execution: The entity authorizing a charging session (fleet orchestrator) should be distinct from the entities executing it (vehicle and charger). This prevents a compromised vehicle or charger from unilaterally initiating or extending sessions. ACAP's three-party JWT model enforces this separation.

B. Limitations

ACAP does not address: (1) fleet-level scheduling optimization across multiple vehicles and stations (an orthogonal problem); (2) bidirectional V2G energy flow, which requires additional grid operator authorization; (3) physical standardization of connector geometries (deferred to CharIN/IEC); (4) regulatory approval processes that vary by jurisdiction. The protocol assumes both vehicle and charger have TPM 2.0 modules, which is not yet universal in deployed charging infrastructure. A migration path using software-based key storage with reduced security guarantees is possible but not specified.

C. Future Work

Priority extensions include: formal verification of the FSM using TLA$^+$ or UPPAAL timed automata; a reference implementation against open-source ISO 15118 stacks (e.g., Josev by Switch-EV); hardware-in-the-loop validation with Rocsys ROC-1 and Tesla wall connector hardware; and integration testing with OCPP 2.1 once ISO 15118-20 support is finalized.

XI. Conclusion

The autonomous charging problem is not fundamentally a hardware problem—robotic arms, wireless pads, and automated connectors all work. It is a *protocol coordination problem*: no standard governs how an autonomous vehicle discovers, authenticates, physically docks with, and transacts with an automated charging station. ACAP fills this gap with a four-phase protocol stack, a 14-state FSM with bounded-time guarantees, Cryptographic Spatial Anchors for relay-resistant positioning, and a fleet-compatible settlement layer. By operating as a companion to ISO 15118-20 and OCPP 2.0.1 rather than replacing them, ACAP provides an incremental adoption path for the heterogeneous ecosystem of AV platforms and charger vendors. As the industry approaches the 2026–2027 inflection point—with Tesla Cybercab production, Waymo's multi-city expansion, and CharIN's ACD standardization converging simultaneously—a protocol like ACAP becomes essential infrastructure for the scalable, secure, fully autonomous charging that robotaxi fleets require.

References

[1] Waymo LLC, "Waymo One: Scaling autonomous ride-hailing," 2024–2026. [Online]. Available: https://waymo.com/waymo-one/

[2] Tesla, Inc., "We, Robot—Cybercab unveil event," Burbank, CA, Oct. 2024; "Cybercab production begins at Giga Texas," Feb. 2026.

[3] Zoox, Inc., "Zoox autonomous vehicle specification," 2024. [Online]. Available: https://zoox.com/vehicle/

[4] ISO, "ISO 15118-20:2022—Road vehicles—Vehicle to grid communication interface—Part 20: 2nd generation network and application protocol requirements," 2022.

[5] Open Charge Alliance, "Open Charge Point Protocol 2.0.1," 2023. [Online]. Available: https://openchargealliance.org/

[6] SAE International, "SAE J3400—NACS Electric Vehicle Coupler," Sep. 2024.

[7] Rocsys B.V., "Autonomous charging of electric vehicles with robotics: How it works," 2023. [Online]. Available: https://www.rocsys.com/technology/

[8] S. Köhler, R. Baker, M. Strohmeier, and I. Martinovic, "Brokenwire: Wireless disruption of CCS electric vehicle charging," in *Proc. NDSS Symposium*, 2023.

[9] S. Köhler *et al.*, "DCeption: Real-world wireless man-in-the-middle attacks against CCS EV charging," arXiv:2601.15515, Jan. 2026.

[10] SAE International, "SAE J3105—Electric vehicle power transfer system using conductive automated connection devices," Jan. 2020.

[11] CharIN e.V., "ACD-U minimum functional requirements whitepaper," v1, Jul. 2025. [Online]. Available: https://www.charin.global/

[12] International Energy Agency, "Global EV Outlook 2024," Paris, 2024.

[13] 3GPP, "Release 16: 5G NR V2X," TS 38.885, 2020.

[14] IEEE, "IEEE 802.15.4z-2020—Enhanced impulse radio," 2020.

[15] Trusted Computing Group, "TPM 2.0 Automotive Thin Profile," v1.1, 2023.

[16] Fraunhofer SIT, "A security analysis of the ISO/IEC 15118 standard," Tech. Rep. SIT-TR-2019-04, 2019.

[17] CISA, "Advisory ICSA-26-057-03: OCPP WebSocket authentication bypass," Feb. 2026.

[18] Terawatt Infrastructure, "Fleet charging solutions for autonomous vehicles," 2025. [Online]. Available: https://www.terawattinfrastructure.com/