Zero Trust Defense Against Charge Manipulation Attacks in Smart EV Charging Infrastructure

Authors: Saba Marandi, Danial Jafarigiv, Ribal Atallah, Mohsen Ghafouri, Chadi Assi

Concordia Institute of Information and Systems Engineering, Concordia University, Montreal, Canada

Presenting by

Saba Marandi
Saba.Marandi@mail.concordia.ca

The Sixteenth International Conference on Smart Grids, Green Communications and IT Energy-aware Technologies
ENERGY 2026

Biography:

Bachelor's 2016-2020	University Of Tabriz Electrical Engineering (Telecommunication)
Master's 2020-2023	Shahid Beheshti University Electrical Engineering (Secure Communication & Cryptology)
Ph.D. 2024-Present	Concordia University Information and System Engineering

Research Interests:

- ✓ electric vehicle charging systems
- ✓ cybersecurity in power systems
- ✓ security and privacy in IoT applications
- ✓ machine learning

Main Outlines

01 **Motivation & Problem Statement**

Growing EV infrastructure and cybersecurity gaps

02 **Threat Model**

Three categories of Charge Manipulation Attacks

03 **Proposed ZTA Framework**

Architecture and system components

04 **Trust Evaluation Model**

Markov-based Stability, Intimacy & Abnormality and update process

05 **Policy Enforcement & OCPP**

PDP/PEP integration with OCPP 2.0.1

06 **Simulation & Results**

Attack detection effectiveness

07 **Conclusions & Future Work**

Scalability, open challenges

1 Motivation & Problem Statement

Rapid Growth

EV charging stations are expanding rapidly in scale and network complexity [1]

Cloud Dependence

Backend management via cloud APIs and remote protocols introduces new attack surfaces [2]

Protocol Risk

OCPP 1.6/2.0.1 protective features can be bypassed with elevated access [3]

Perimeter Failure

Traditional boundary-based models cannot protect dynamic, distributed EVCS [4]

Key Challenge

- No session-level protocol enforcement
- Static trust with no real-time updates
- No charger-side behavioral detection
- OCPP misuse goes undetected
- Evolving threats bypass perimeter

2 Threat Model: Charge Manipulation Attacks

Adversaries possess moderate-to-advanced resources including access to compromised credentials, mobile apps, and backend interfaces [5,6].

DEMAND SURGE

- Simultaneously initiate large-scale charging
- Destabilizing grid demand spikes
- Man-in-the-Middle session injection
- Exploits weak/static authentication

COORDINATED SWITCHING

- Periodic on/off cycling of chargers
- Triggers inter-area oscillations
- Concealed via FDIA on telemetry
- Uses tampered firmware/scheduler

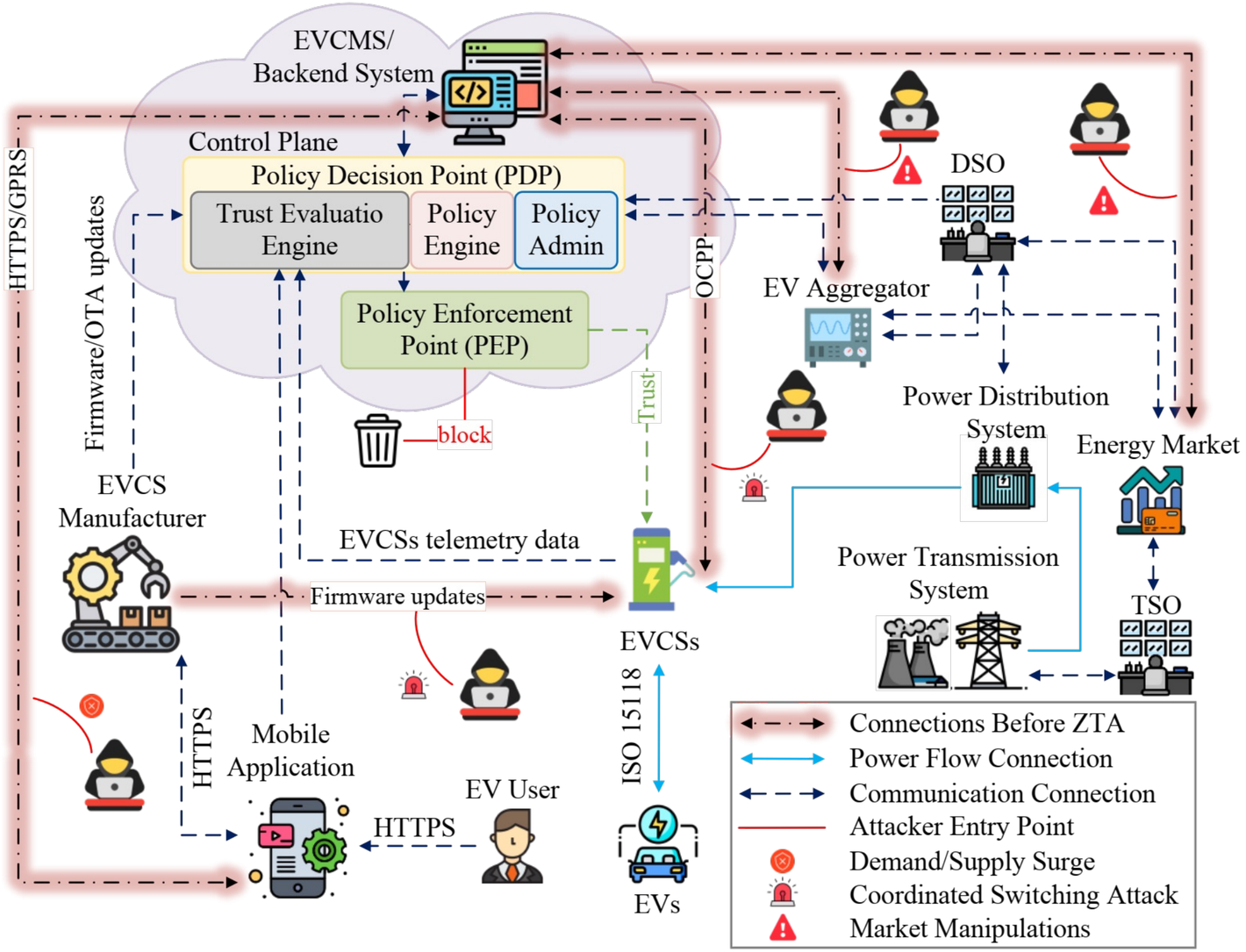
MARKET MANIPULATION

- Distort price signals and trading
- Inject false load data into aggregators
- Exploit EVCMS or aggregator APIs
- Spoofed measurement values

All attack types exploit protocol weaknesses and can bypass perimeter-based security → ZTA is required

3 Proposed ZTA Framework: System Architecture

Core Principle:
No charging request is trusted by default
every interaction is evaluated in real-time based on behavioral context, device integrity, and protocol activity.



4 Trust Evaluation: Three Behavioral Dimensions

Stability Degree (SD)

Weight: 0.4

Evaluates consistency of charger communication connection disruptions and request timeouts

$$T_s^{(t)} = T_s^{(t-1)} + ((V_l + \lambda_l \cdot l_s) \cdot (T_l - l_s)) + ((V_r + \lambda_r \cdot r_s) \cdot (T_r - r_s))$$

- l_s, r_s = connection disruptions, request timeouts
- V_l, V_r = penalty weight for connection disruptions/request timed out
- T_l, T_r = maximum allowable threshold for distruption/timeouts
- Rapid penalty when thresholds exceeded

Intimacy Degree (ID)

Weight: 0.3

Quantifies historical interaction strength between charger and cloud management platform

$$T_i^{(t)} = T_i^{(t-1)} + (q_i + \eta_1 R_t + \eta_2 R_t')(R_t' - R_t)$$

- R_t = percentile rank of interaction
- q_i = fluctuation control parameter (moderates sensitivity to minor rank changes)
- Decreased activity → reduced trust
- Stable/improved frequency → accumulation

Abnormality Degree (ED)

Weight: 0.3

Captures deviations: protocol misuse, unauthorized commands, geographic inconsistencies

$$T_e^{(t)} = \begin{cases} T_e^{*(t)} + \sum_{i=1}^{N} Q(\text{Exception}_i), & N \neq 0 \\ T_e^{*(t)} - p_e, & N = 0 \end{cases}$$

- $Q(.)$ = severity score per anomaly
- p_e = recovery coefficient
- Fine-grained contextual penalization

Global Trust Score: $T_n^{(t)} = w_s \cdot T_s^{(t)} + w_i \cdot T_i^{(t)} - w_e \cdot T_e^{(t)}$ where $w_s + w_i + w_e = 1$

4 Markov-Based State Update Process

Each trust dimension is modeled as a discrete-time Markov chain with 5 trust states, enabling probabilistic prediction of charger behavior.

Bayesian Belief Update

$$\pi_d^{(t)} = \frac{P_d^\top \cdot \left(\pi_d^{(t-1)} \odot \mathcal{O}_d(z_d^{(t)})\right)}{\left\| P_d^\top \cdot \left(\pi_d^{(t-1)} \odot \mathcal{O}_d(z_d^{(t)})\right) \right\|_1}$$

$\boldsymbol{\pi_d^{(t)}}$ = belief distribution over 5 states
p_d = stationary Markov transition matrix
$\boldsymbol{O_d(z_d^{(t)})}$ = observation likelihood vector

Trust Score Computation & Authorization

$$T_d^{(t)} = \pi_d^{(t)} \cdot \mathbf{v}_d$$

$$\mathbf{v}_d = [0.0, 0.25, 0.5, 0.75, 1.0]^\top$$

Each 3-hour evaluation window updates all trust dimensions.
Authorization decision:

$$K_n^{(t)} = JWT\ issued\ if\ T_n^{(t)} \geq \tau\ (threshold = 70)$$

5 Policy Enforcement & OCPP 2.0.1 Integration

Policy Enforcement Point (PEP) Workflow

1. Intercept OCPP 2.0.1 request from EVCS
2. Parse message & inspect embedded JWT token
3. Verify scope, expiration & signature integrity
4. Check $r_i^{(t)} \in \mathscr{A}(\mathscr{P}, \kappa)$ → allowable actions
5. Accept or block & flag mismatch
6. Validated the token and request $\mathrm{Verify}(\sigma_{\mathrm{firm}}, K_{\mathrm{pub}}^{\mathrm{PDP}}) = \mathtt{True}$

Key Properties & OCPP Controls

- All EVCS messages routed through PEP
- JWT: short-lived, cryptographically signed
- Session-level verification per request
- The request requires PDP authorization
- Digital signature check before the implementation of command
- Context-aware enforcement for CMAs

Only chargers with $T_n^{(t)} \geq \tau$ receive access tokens

6 Simulation Setup & Methodology

Chargers	Evaluation Windows	Attack Rate	Protocol
5 (A–E)	**10**	**30%**	**OCPP 2.0.1**
Real-world dataset 2 outlets each	Each = 3-hour peak period	Sessions injected with CMA	Python emulation All messages valid

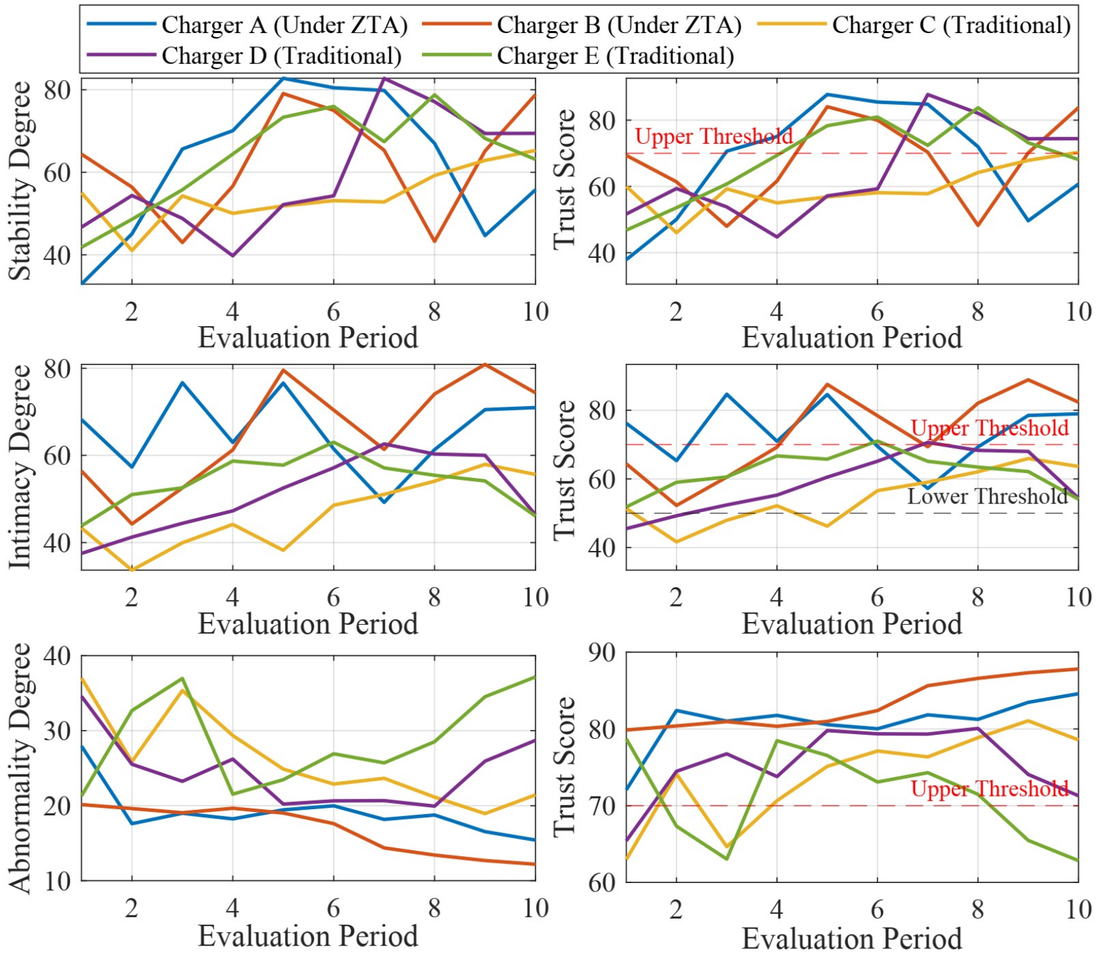
TRUST LEVEL HIERARCHY

Trust Level	Controlling Measure	Permission	Trust Score Range
I	N/A	Monitored access	[90,100]
II	Downgrading permissions	Restricted access; Monitored access	[70,90)
III	Re-authenticating	Access temporarily denied	[50,70)
IV	Blocking connections	Access denied	[0,50)

Attack Injection Strategy

- Modified: energy requested & charging duration
- Syntactically on valid OCPP 2.0.1 messages
- Randomized across chargers & time windows
- Mimics stealthy, coordinated behavior
- Designed to evade rule-based detection

6 Results: Trust Score Evolution Under Attack



ZTA Observation (A & B)

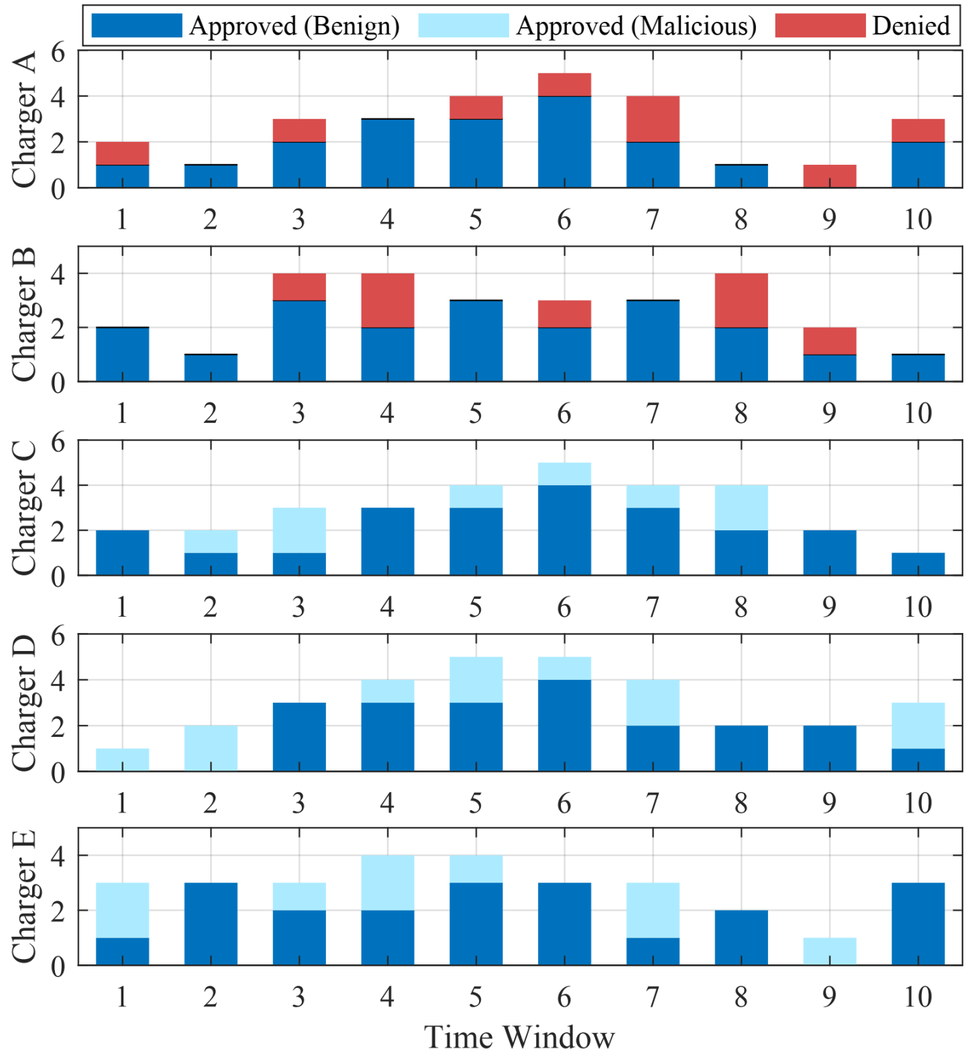
Sessions denied when trust drops below Level II threshold (≥70). Proactive access control prevents attack propagation.

Traditional Observation (C, D, E)

Trust score degrades similarly, but no enforcement occurs→all sessions, including malicious ones are approved regardless of behavioral anomalies.

ZTA enforcement threshold (τ = 70) separates Trust Level II from Level III — triggering re-authentication or denial.

6 Results: Access Control Effectiveness and Computational Overhead & Scalability



ACCESS CONTROL EFFECTIVENESS UNDER CMA

Charger Type	Approved	Denied	Denial Rate
A (ZTA-enabled)	19	8	100%
B (ZTA-enabled)	20	7	87.5%
C (Traditional)	30	0	0.0%
D (Traditional)	31	0	0.0%
E (Traditional)	29	0	0.0%

Key Finding

ZTA-enabled chargers blocked 87.5–100% of malicious sessions.
Traditional chargers approved 100% regardless of attack.

Trust Score Update (per charger)	JWT Token Verification (PEP)	Session Init Latency
120–150 ms	**2–5 ms**	**Seconds**
Every 3-hour window Intel Xeon E5-2680 v4, 8 GB RAM	Per session request Signature validation overhead	Token overhead negligible vs. typical session timing

7 Conclusion

Novel ZTA Framework

Continuous behavioral assessment of EVCS with dynamically issued trust tokens based on real-time indicators

Markov-Based Trust Model

State-aware probabilistic tracking of Stability, Intimacy & Abnormality dimensions across 5 trust states

OCPP 2.0.1 Integration

Session-level enforcement via PEP with JWT tokens; firmware validated by PEP before OTA deployment

Validated Effectiveness

87.5–100% malicious session detection vs. 0% for traditional models under coordinated CMA scenarios

References

1. “Global EV Outlook 2024 – Analysis - IEA,” IEA, April 2024. [Online]. Available: https://www.iea.org/reports/global-ev-outlook-2024
2. 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 Natl. Lab., Albuquerque, NM (US), Tech. Rep., 2022
3. K. KSarieddine, M. A. Sayed, C. Assi, R. Atallah, S. Torabi, J. Khoury, M. S. Pour, and E. Bou-Harb, “Ev charging infrastructure discovery to contextualize its deployment security,” IEEE Transactions on Network and Service Management, vol. 21, no. 1, pp. 1287–1301, 2024.
4. T. E. Carroll, L. H. Chang, and C. L. Wright-Hamor, “The design and evaluation of zero trust architecture for electric vehicle charging infrastructure: Evs@ scale series on ev charging station cybersecurity,” Pacific Northwest National Laboratory (PNNL), Richland, WA (United States), Tech. Rep., 2024.
5. H. Jahangir, S. Lakshminarayana, and H. V. Poor, “Charge manipulation attacks against smart electric vehicle charging stations and deep learning- based detection mechanisms,” IEEE Transactions on Smart Grid, 2024.
6. M. Bampatsikos, I. Politis, T. Ioannidis, and C. Xenakis, “Trust score prediction and management in iot ecosystems using markov chains and madm techniques,” IEEE Transactions on Consumer Electronics, 2025.

THANKS

FOR YOUR ATTENTION

CONTACT

SCAN ME

SCAN ME