Timed Command Interference: A Timing-Based DoS Attack on Grid-Integrated EV Scheduling

1st Saba Marandi
CIISE Department
Concordia University
Montreal, Canada
saba.marandi@mail.concordia.ca

2st Mohammad Mahdi Soleymani
CIISE Department
Concordia University
Montreal, Canada
mahdsoleymani@gmail.com

3st Danial Jafarigiv
Digitization & Cybersecurity, R&D Department
Hydro-Québec Research Institute
Varennes, Canada
jafarigiv.danial2@hydroquebec.com

4st Ribal Atallah
Digitization & Cybersecurity, R&D Department
Hydro-Québec Research Institute
Varennes, Canada
atallah.ribal@hydroquebec.com

5th Mohsen Ghafouri
CIISE Department
Concordia University
Montreal, Canada
mohsen.ghafouri@concordia.ca

6th Chadi Assi
CIISE Department
Concordia University
Montreal, Canada
chadi.assi@concordia.ca

***Abstract*—This paper presents Timed Command Interference (TCI), a novel timing-based denial-of-service (DoS) attack that exploits the tight temporal coupling between communication delays and grid dynamics in Electric Vehicle (EV) scheduling systems. Unlike flooding-based DoS attacks that saturate network capacity, TCI injects strategic timing delays in control commands between the Distribution System Operator (DSO) and distributed EV aggregators, causing temporal misalignment between optimized schedules and their physical execution. By manipulating command timing rather than data volume, TCI destabilizes voltage regulation and power balance even when the DSO's optimization is mathematically correct. Three attack strategies, including staggered delay, peak-synchronized interference, and cascading timeout, are modeled using a hybrid cyber-physical framework that integrates delay dynamics with AC optimal power flow. Simulations on a modified IEEE-33-bus network with realistic EV charging profiles show that TCI increases voltage deviations by 76% and scheduling costs by 5.3% while consuming less than 1% of traditional distributed DoS (DDos) bandwidth. The results reveal the first systematic timing-layer vulnerability in EV scheduling coordination and highlight the need for temporal authentication and redundant execution-verification mechanisms to ensure grid-level resilience.**

***Index Terms*—EV scheduling, DoS, Smart Grid Resilience, cyber-physical security, Timing Synchronization**

I. Introduction

The electrification of transportation has accelerated the deployment of electric vehicle (EV) charging infrastructure, with projections indicating over 30 million EVs on roads by 2030 [1]. Managing this substantial load presents critical coordination challenges for power distribution networks, as large-scale EV integration fundamentally reshapes grid operations and requires advanced scheduling mechanisms to preserve system stability [2]. When EV charging occurs without proper coordination, distribution systems experience voltage profile degradation, thermal overloading of network components, and congestion at critical nodes [3]. This creates an urgent need for optimization frameworks that harmonize charging demand with operational constraints at the distribution level. In response to these challenges, Distribution System Operators (DSOs) have adopted centralized optimization-based command-and-control paradigms wherein optimal charging schedules are computed through mathematical programming at a control center and subsequently transmitted as time-stamped executable commands to geographically dispersed EV aggregators [4]. The effectiveness of this coordination approach relies on maintaining precise temporal synchronization between the time the optimization solver generates schedules and the moment the aggregators execute them. This dependency forms a critical cyber-physical coupling whose security implications remain largely unexplored.

Recent research highlights that the growing digitalization of EV charging coordination has expanded its cybersecurity attack surface. Most prior studies have examined high-volume and data-integrity threats, such as Distributed Denial-of-Service (DDoS) attacks that saturate communication channels [5] and False Data Injection Attacks (FDIAs) that distort control signals and state estimation in smart grids [6]. Defensive efforts against these attacks have primarily relied on observer-based [7] and machine-learning-based [8] anomaly detection techniques. However, these approaches overlook a subtle but important threat, where an attacker can coordinate small timing delays across several communication links to cause much larger effects on the grid. Unlike conventional DoS attacks that rely on overwhelming traffic, selective timing manipulation can destabilize EV scheduling while remaining largely invisible to monitoring systems. This overlooked attack vector exposes a critical weakness in optimization-driven EV coordination, which depends heavily on precise timing between decision and execution. The vulnerability arises because EV scheduling creates exploitable temporal coupling through sub-second synchronization, far tighter than traditional SCADA systems that operate on minute-scale control loops [9]. When a DSO computes an optimal charging schedule that enforces bus-level voltage limits, even slight timing misalignments between the intended schedule and its actual execution can cascade into measurable grid violations. Unlike conventional power systems, where generation and demand evolve gradually, EV charging introduces rapid power variations due to high-power fast charg-

979-8-3315-8138-1

ing and bidirectional Vehicle-to-Grid (V2G) operations [10]. Recent work has examined how adversaries manipulate IoT-enabled devices to disrupt power grids [11], and research has identified control-related vulnerabilities in EV systems [12]; however, these studies primarily address data integrity and authentication failures rather than the exploitation of temporal coordination dependencies. Prior studies on cascading failures have shown how cyberattacks launched at multiple points can trigger successive component outages and lead to large-scale blackouts [13]. However, the specific mechanism by which temporal command delays translate into physical grid violations in EV scheduling systems has not yet been investigated.

To address these gaps, this paper introduces Timed Command Interference (TCI), a novel timing-based DoS attack exploiting temporal coordination vulnerabilities in EV scheduling. Unlike bandwidth-saturating attacks, TCI manipulates only command delivery timing to desynchronize aggregator execution, causing grid violations while evading volume-based detection. Our contributions are threefold: First, we formalize three coordinated TCI strategies—staggered delay, peak-synchronized interference, and cascading timeout—that maximize grid impact with minimal bandwidth. Second, we develop a cyber-physical framework integrating delay dynamics with AC power flow to quantify timing perturbations' propagation into voltage and cost impacts. Third, we introduce quantification metrics (VDI, NCI), enabling systematic attack effectiveness comparison. Simulations on the IEEE 33-bus system show TCI achieves 76% higher voltage deviation and 5.3% cost increase versus random failures $< 1\%$ DDoS bandwidth, establishing timing manipulation as a critical attack vector for cyber-physical systems.

II. System Model and Attack Framework

A. EV Charging System Architecture

The EV charging ecosystem comprises four hierarchical components: EVs, EV Charging Stations (EVCS), EV Aggregators (Agg), and the DSO. As illustrated in Fig. 1, the physical layer establishes power flow connections between EVs and the distribution grid through charging stations, while the cyber layer enables bidirectional communication between the DSO control center and aggregators via wired/wireless networks. Each aggregator $i \in \mathcal{N} = \{1,2,...,N\}$ coordinates multiple charging stations within a geographical region, distributing charging commands computed by the DSO to maintain grid-level voltage stability and minimize distribution losses.

B. Centralized Scheduling Optimization Framework

The DSO formulates a multi-period optimization problem to coordinate EV aggregator charging/discharging schedules across the planning horizon while enforcing distribution network operational constraints. The optimization objective seeks to minimize the aggregate cost comprising grid energy procurement and resistive distribution losses adopted from [14], [15]:

$$\min_{\mathbf{P}} \sum_{t=1}^{T} \left(C_{\text{grid}}(t) \sum_{i=1}^{N} P_i(t) + \lambda \sum_{\ell=1}^{L} P_{\text{loss},\ell}(t) \right) \tag{1}$$

where $C_{\text{grid}}(t)$ denotes the time-varying grid electricity price, $P_i(t)$ represents the net power injection/withdrawal of aggregator i at time slot $t \in \{1,2,...,T\}$, $P_{\text{loss},\ell}(t)$ captures resistive

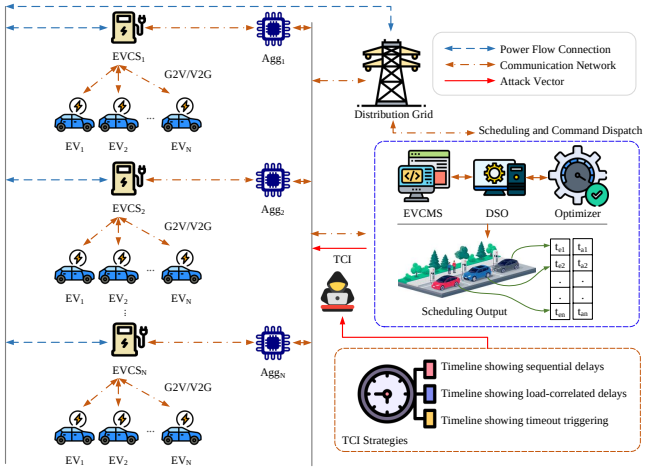

Fig. 1: EV scheduling system architecture with TCI attack injection points.

losses at distribution line ℓ (calculated as $|I_\ell(t)|^2 R_\ell$ where $I_\ell(t)$ is line current and R_ℓ is resistance), and λ is the economic weight assigned to loss minimization. Voltage $V_j(t)$ at each bus j is determined implicitly through AC power flow equations given power injections/absorption P. The optimization is subject to the following technical constraints:

$$P_{\text{sub}}(t) = \sum_{i=1}^{N} P_i(t) + \sum_{\ell=1}^{L} P_{\text{loss},\ell}(t) \tag{2}$$

$$V_j^{\min} \le V_j(t) \le V_j^{\max}, \quad \forall j \in \mathcal{B} \tag{3}$$

$$\underline{P}_i(t) \le P_i(t) \le \overline{P}_i(t) \tag{4}$$

$$\text{SoC}_i^{\min} \le \text{SoC}_i(t) \le \text{SoC}_i^{\max}, \quad \forall i,t \tag{5}$$

where the state-of-charge evolves according to:

$$\text{SoC}_i(t+1) = \text{SoC}_i(t) + \frac{\eta_{\text{ch}} P_i^+(t) \Delta t}{E_i^{\text{cap}}} - \frac{P_i^-(t) \Delta t}{\eta_{\text{dch}} E_i^{\text{cap}}} \tag{6}$$

for all $t \in \mathcal{T}$, $i \in \mathcal{N}$, where $P_{\text{sub}}(t)$ denotes the substation power injection at the grid interface, $P_i(t)$ represents the net aggregate power of aggregator i, $P_{\text{loss},\ell}(t)$ captures resistive losses at distribution line ℓ, $V_j(t)$ is the voltage magnitude at bus j, $\underline{P}_i(t)$ and $\overline{P}_i(t)$ represent the time-varying minimum and maximum power limits for aggregator i, $\text{SoC}_i(t)$ is the aggregate state-of-charge of the EV fleet managed by aggregator i, $P_i^+(t)$ and $P_i^-(t)$ denote aggregate charging and discharging power of aggregator i respectively, E_i^{cap} is the total aggregated battery capacity of aggregator i's fleet, η_{ch} and η_{dch} are charging and discharging efficiencies, Δt is the time step duration, $\mathcal{T} = \{1,2,...,T\}$ is the set of time slots, $\mathcal{N} = \{1,2,...,N\}$ is the set of aggregators, $\mathcal{B} = \{1,2,...,B\}$ is the set of distribution buses, and $\mathcal{L} = \{1,2,...,L\}$ is the set of distribution lines.

The optimal EV scheduling problem with AC power flow constraints is non-convex due to nonlinear voltage-power coupling, making exact solutions computationally intractable. We employ an iterative heuristic approach [16] in which the DSO first computes candidate charging schedules based on time-of-use pricing while respecting power and SoC constraints (Eqs. 4-6), then validates voltage feasibility using forward-backward sweep power flow analysis for radial networks. If voltage vio-

lations occur (Eq. 3), charging powers are scaled proportionally and iteratively re-validated until feasibility is achieved. While not guaranteeing global optimality—a fundamental limitation of non-convex AC-OPF—this method provides computationally efficient near-optimal solutions suitable for real-time operation, with effectiveness validated through Monte Carlo simulation. The DSO solves this optimization problem to obtain the optimal power schedules $\mathbf{P}^* = [P_1^*(t), ..., P_N^*(t)]$ for all $t \in \mathscr{T}$ and transmits time-stamped control commands $\mathscr{C}_i(t) = \{P_i^*(t), t_{\text{exec}}\}$ to each aggregator i, where t_{exec} specifies the precise execution timestamp for time slot t.

C. Timed Command Interference (TCI) Attack Model

1) Attack Mechanism and Threat Model: The TCI attack exploits the temporal dependency between schedule computation and physical execution by strategically delaying DSO control commands to selected aggregators. Unlike conventional DoS attacks that flood the network with volumetric traffic, TCI operates through precise timing manipulation that consumes minimal bandwidth and remains below volume-based intrusion detection thresholds. We assume the attacker has compromised aggregator-side communication infrastructure (e.g., protocol gateways, cellular modems, or SCADA interfaces), as illustrated in Fig. 1. Such access is achievable through phishing attacks, SCADA vulnerability exploitation, or physical access to remote equipment. The attacker possesses: (1) passive observation of command traffic patterns to learn scheduling cycles and message structures, (2) message interception capability via man-in-the-middle positioning, using ARP spoofing, DNS hijacking, or compromised firmware, and (3) controlled delay injection by holding intercepted packets in a buffer queue before forwarding, implemented through traffic shaping rules in iptables/tc or similar packet manipulation tools. Importantly, the attacker cannot decrypt or modify command content, nor can it generate valid cryptographic signatures. The attack manipulates only the physical-layer delivery timing by strategically releasing buffered messages at calculated intervals, without altering message content or cryptographic properties. Upon intercepting control command $\mathscr{C}_i(t) = \{P_i^*(t), t_{\text{exec}}\}$ destined for aggregator i, the attacker introduces a calculated delay $\delta_i(t)$ before forwarding the unmodified command:

$$t_{\text{actual}} = t_{\text{exec}} + \delta_i(t) \tag{7}$$

where t_{actual} denotes the actual execution time experienced by the aggregator. The delay magnitude $\delta_i(t)$ is strategically chosen based on the attack strategy (detailed in Section II-C2) to maximize grid impact while maintaining stealth.

The delayed execution creates temporal misalignment between the DSO's expected grid state (computed assuming execution at t_{exec}) and the actual physical state (manifested at t_{actual}). This desynchronization causes grid constraint violations despite mathematically correct optimization, as the power flow equations evolve differently than anticipated:

$$V_j(t_{\text{actual}}) \neq V_j^{\text{expected}}(t_{\text{exec}}), \quad \forall j \in \mathscr{B} \tag{8}$$

when multiple aggregators experience coordinated delays, the cumulative effect cascades through the distribution network, potentially triggering voltage limit violations (3) (0.95-1.05 p.u. as per IEEE 1547 standard) and substation capacity violations.

2) Attack Strategies: We formalize three distinct TCI attack strategies that exploit different temporal vulnerabilities in the scheduling coordination process:

Staggered Delay Attack: This strategy sequentially targets aggregators with progressively increasing delays to create spatial desynchronization across the distribution network:

$$\delta_i(t) = \begin{cases} \Delta \cdot (i - \min(\mathscr{N}_{\text{target}})), & \text{if } i \in \mathscr{N}_{\text{target}} \\ 0, & \text{otherwise} \end{cases} \tag{9}$$

where Δ is the base delay increment measured in scheduling intervals, and $\mathscr{N}_{\text{target}} \subseteq \mathscr{N}$ represents the set of targeted aggregators. This creates a cascading wave of temporally staggered executions where aggregator i executes its schedule Δ time slots later than aggregator $(i-1)$, amplifying voltage imbalances as delayed power injections accumulate spatially along the radial feeder.

Peak-Synchronized Interference: This strategy amplifies delays during high-demand periods when the grid is most vulnerable to disturbances:

$$\delta_i(t) = \begin{cases} \Delta_{\max} \cdot \frac{P_{\text{sub}}(t)}{P_{\text{sub}}^{\max}}, & \text{if } i \in \mathscr{N}_{\text{target}} \text{ and } t \in \mathscr{T}_{\text{peak}} \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

where $\Delta_{\max}$ is the maximum allowable delay, $P_{\text{sub}}(t)$ is the substation loading at time t, $P_{\text{sub}}^{\max}$ is the substation capacity, and $\mathscr{T}_{\text{peak}}$ denotes time slots where $P_{\text{sub}}(t) \geq 0.8 \cdot P_{\text{sub}}^{\max}$. By scaling delays proportionally to grid stress, this strategy maximizes the likelihood of constraint violations during periods when voltage margins are already reduced.

Cascading Timeout Attack: This strategy induces communication timeouts that force aggregators into uncoordinated fallback operating modes:

$$\delta_i(t) = \begin{cases} \tau_{\text{timeout}} + \varepsilon, & \text{with probability } p_{\text{attack}},\ i \in \mathscr{N}_{\text{target}} \\ 0, & \text{otherwise} \end{cases} \tag{11}$$

where τ_{timeout} is the communication timeout threshold (typically 2-5 seconds for SCADA systems), $\varepsilon > 0$ is a small margin ensuring reliable timeout triggering, and $p_{\text{attack}} \in [0,1]$ controls attack frequency. When timeouts occur, aggregators typically revert to default charging modes (e.g., immediate full-power charging) that disregard grid constraints, causing uncoordinated load spikes that destabilize voltage profiles.

D. Attack Impact Quantification

To systematically evaluate TCI effectiveness, we define two complementary metrics that capture physical grid degradation and economic consequences:

Voltage Deviation Index (VDI): It quantifies the cumulative departure from nominal voltage across all buses and time periods:

$$\text{VDI} = \frac{1}{|\mathscr{B}| \cdot T} \sum_{t=1}^{T} \sum_{j \in \mathscr{B}} \left| V_j(t) - V_j^{\text{nom}} \right| \tag{12}$$

where V_j^{nom} is the nominal voltage at bus j (typically 1.0 per-unit). Higher VDI values indicate greater voltage instability induced by the attack.

Normalized Cost Increase (NCI): It measures the economic impact of timing manipulation relative to optimal operation:

$$\text{NCI} = \frac{C_{\text{attack}} - C_{\text{optimal}}}{C_{\text{optimal}}} \times 100\% \tag{13}$$

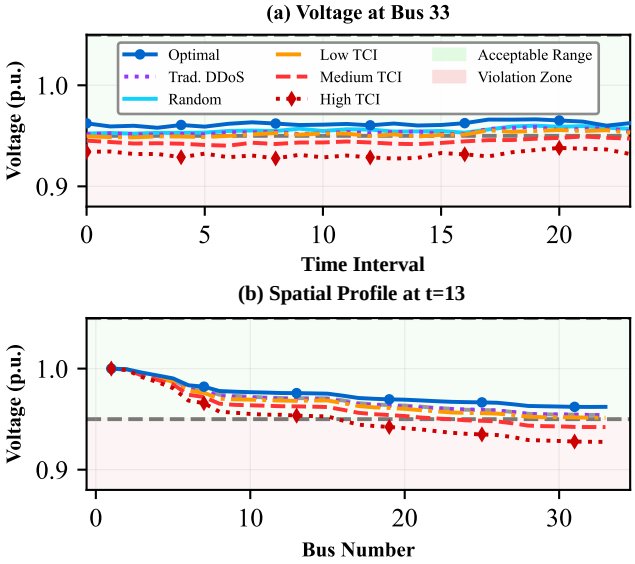

Fig. 2: Voltage profiles under cyberattacks: (a) Temporal evolution at Bus 33, (b) Spatial distribution at peak interval.

where C_{attack} represents the total operational cost (grid procurement + losses) when the system operates under TCI attack, and C_{optimal} is the cost achieved under uncompromised optimal scheduling. This metric captures both direct costs (increased grid purchases due to suboptimal timing) and indirect costs (higher resistive losses from voltage deviations).

III. Case Study and Result Analysis

A. Simulation Configuration

We evaluate TCI effectiveness on a modified IEEE 33-bus distribution network (12.66 kV) with 6 EV aggregators positioned at buses 5, 10, 15, 20, 25, and 30, managing 3,450 kWh total capacity (≈70-85 EVs with 40-50 kWh batteries, 7.2 kW Level 2 AC charging with bidirectional V2G capability). The system employs realistic AC power flow with cumulative radial topology modeling, incorporating line resistance, reactance, and reactive power (pf=0.95). Monte Carlo simulation (50 runs) uses time-of-use pricing with five tiers reflecting typical utility rate structures: off-peak ($0.05/kWh), mid-peak morning ($0.12/kWh), standard ($0.09/kWh), peak evening ($0.16/kWh), and off-peak night ($0.07/kWh). Four attack scenarios are tested: **Random Delay** (40% aggregators receive commands delayed by 1-2 scheduling slots, baseline), **Low-Intensity TCI** (3 aggregators with progressive staggered execution shifts of 1-3 time slots), **Medium-Intensity TCI** (4 aggregators with staggered slot delays of 1-4 intervals plus peak-synchronized interference on 3 aggregators during high-stress periods), **High-Intensity TCI** (full coordination: 4 aggregators with staggered delays + 5 with peak-synchronized interference + 2 experiencing cascading timeouts with $p_{\text{attack}} = 0.20$). Traditional DDoS (40% command delivery failure) provides a comparative baseline.

B. Voltage Impact and Attack Mechanisms

Fig. 2(a) reveals that coordinated TCI attacks cause escalating voltage violations at Bus 33. High-intensity TCI depresses voltage to 0.927–0.938 p.u., with minimum voltage 0.927 p.u. at $t = 13$, which is a 3.47% deviation below optimal voltage value (0.962 p.u.). Medium-intensity attacks maintain voltage at 0.940–0.949 p.u., while low-intensity TCI operates at 0.948–0.956 p.u., with violations occurring during 24, 24, and 9 intervals, respectively. The violations occur when delayed aggregator executions create uncoordinated power injections that compound cumulative power flow imbalances along the radial feeder. Critically, optimal scheduling maintains stable voltage at 0.958–0.966 p.u. throughout all periods, demonstrating that coordinated timing manipulation invalidates mathematically correct optimization. Traditional DDoS and random delays cause no violations at Bus 33 (0.951–0.959 p.u. and 0.952–0.960 p.u. respectively), despite DDoS consuming 100× more bandwidth than TCI attacks. This validates that coordinated timing strategies achieve more severe grid destabilization than conventional volumetric attacks.

The spatial profile (Fig. 2b) at peak interval (t=13, 96.3% substation loading) shows voltage decaying from 1.0 p.u. (Bus 1) to 0.962 p.u. (Bus 33) under optimal operation—a 3.8% drop along the radial feeder. High-intensity TCI amplifies this degradation to 0.927 p.u. at Bus 33, resulting in a 7.3% total voltage drop and a 92% increase in the severity of the voltage gradient. The voltage decay exhibits nonlinear intensification beyond Bus 15, where high-impedance feeder sections exacerbate downstream voltage drops under concentrated power flow. This demonstrates that remote bus targeting exploits cumulative power flow amplification: delays at distant aggregators create both local injection misalignment and upstream flow disruption, compounding voltage stress through dual mechanisms absent in random failures.

C. Quantitative Assessment and Attack Characterization

Table I quantifies that high-intensity TCI achieves VDI=0.0466 ± 0.0002 p.u. (76% increase) and NCI=5.27% ± 0.82%, establishing reproducible severe impact (tight σ) across stochastic variations. The 5.27% cost increase comprises: (1) direct costs from temporal misalignment forcing suboptimal charging during high-price periods (≈3%), (2) indirect resistive loss escalation from voltage imbalances (≈1.5%), and (3) voltage penalty violations triggering operational constraints (≈0.8%). Medium-intensity yields 45% VDI increase and 1.52% NCI, confirming partial coordination effectiveness while potentially evading severity-based detection. Low-intensity produces 25% voltage and 0.63% cost increases—modest but persistent impacts suitable for prolonged stealthy campaigns. Traditional DDoS achieves only 20% VDI increase and 0.30% NCI, demonstrating TCI's 18× economic superiority (5.27% vs. 0.30%) despite $< 1\%$ relative bandwidth consumption—validating that exploiting temporal dependencies dominates volumetric saturation.

Fig. 3 statistical distributions reveal narrow interquartile ranges (IQR ≈ 0.0002–0.0003 p.u. for VDI, $< 1\%$ for NCI at

TABLE I: Coordinated TCI Attack Impact on IEEE 33-Bus System with Realistic AC Power Flow (50 Monte Carlo Runs)

Scenario	VDI (p.u.)	NCI (%)
Optimal	0.0265 ± 0.0001	0.00 ± 0.00
Traditional DDoS	0.0318 ± 0.0002	0.30 ± 0.43
Random Delay	0.0305 ± 0.0001	0.12 ± 0.07
Low-Intensity TCI	0.0331 ± 0.0001	0.63 ± 0.06
Medium-Intensity TCI	0.0383 ± 0.0001	1.52 ± 0.08
High-Intensity TCI	0.0466 ± 0.0002	5.27 ± 0.82

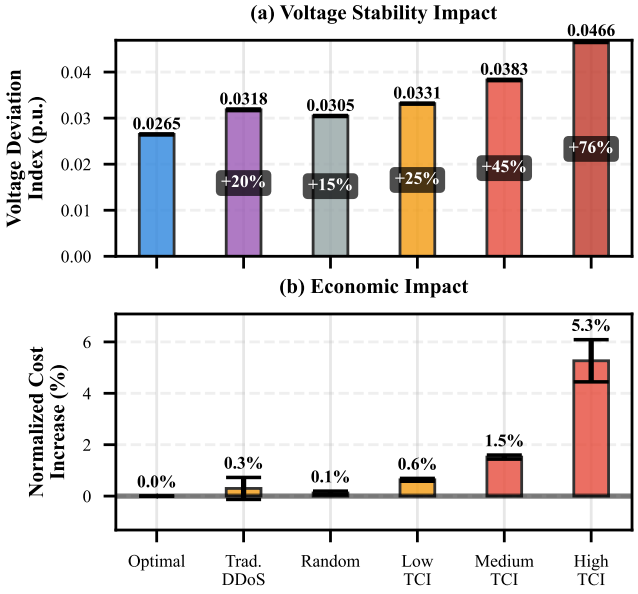

Fig. 3: Impact of different cyber-attack scenarios on the system: (a) Voltage Stability, (b) Economic Cost.

low/medium intensity), confirming consistent attack outcomes across diverse operational conditions with minimal outliers. The progression from low (25% VDI increase) through medium (45%) to high-intensity (76% VDI increase) demonstrates *multiplicative amplification* rather than linear addition: combining staggered delays with peak-synchronized interference yields 1.8× impact over staggered alone, while adding cascading timeouts escalates to 3.0× total impact. This nonlinear escalation exploits compounding grid vulnerabilities, particularly evident during peak loading periods (88–96% substation capacity) where minor delays trigger exponential violation escalation. The cost distribution bimodality at medium intensity (2.8–3.1% range) reflects sensitivity to these stochastic loading variations, revealing sharp nonlinear vulnerability boundaries in constrained grid operation. Crucially, sub-second delays invalidate optimization guarantees despite mathematically correct DSO computation, exposing a fundamental gap between control-theoretic optimality and cyber-physical execution feasibility that cannot be prevented through optimization alone.

TCI's superiority stems from exploiting undefended temporal dependencies in current security frameworks. Traditional DDoS proves limited (0.30% NCI) because distributed EV scheduling systems inherently possess message redundancy and aggregator-level autonomy—when communication fails, aggregators revert to locally cached schedules or safe fallback modes. Paradoxically, this architectural resilience, designed specifically to counter volumetric threats, creates vulnerability to timing manipulation where cached schedules executed at incorrect timestamps produce worse outcomes than communication failure itself. Unlike FDIAs requiring cryptographic key compromise or sophisticated model-based attack construction, TCI operates by intercepting and delaying legitimate DSO-signed control messages without modification, bypassing security frameworks that verify message integrity and origin but neglect temporal consistency validation between intended execution timestamps and actual arrival times.

IV. Conclusion

This paper introduced Timed Command Interference (TCI), a novel timing-based attack exploiting temporal coordination vulnerabilities in EV scheduling systems, demonstrating that temporal delay injection achieves 76% voltage degradation and 5.3% cost increase at $< 1\%$ DDoS bandwidth through strategic desynchronization of DSO-computed optimal schedules. The attack's effectiveness stems from exploiting tight cyber-physical coupling, where timing misalignment invalidates optimality despite correct mathematical computation, revealing that distributed coordination systems face fundamental vulnerabilities when adversaries synchronize timing disruptions across spatially separated components. Future work should investigate temporal authentication mechanisms validating message arrival timing consistency, execution-verification protocols detecting schedule-execution misalignment through predicted-versus-measured state cross-validation, and distributed resilient architectures maintaining partial coordination under communication disruptions to ensure grid-level resilience against timing-layer attacks.

References

[1] International Energy Agency. (2024) Global EV Outlook 2024. https://www.iea.org/reports/global-ev-outlook-2024. Licence: CC BY 4.0, Accessed: ctober 14, 2025.

[2] E. Balogun *et al.*, "Ev-ecosim: A grid-aware co-simulation platform for the design and optimization of electric vehicle charging infrastructure," *IEEE Trans. on Smart Grid*, vol. 15, no. 3, pp. 3114–3125, 2023.

[3] P. Dahiwale *et al.*, "A comprehensive review of smart charging strategies for electric vehicles and way forward," *IEEE Trans. on Intelligent Transportation Systems*, vol. 25, no. 9, pp. 10 462–10 482, 2024.

[4] A. Selim *et al.*, "Adaptive deep reinforcement learning algorithm for distribution system cyber attack defense with high penetration of ders," *IEEE Trans. on Smart Grid*, vol. 15, no. 4, pp. 4077–4089, 2023.

[5] K. Sarieddine *et al.*, "Investigating the security of ev charging mobile applications as an attack surface," *ACM Trans. on Cyber-Physical Systems*, vol. 7, no. 4, pp. 1–28, 2023.

[6] T. Huang *et al.*, "Cyber-resilient automatic generation control for systems of ac microgrids," *IEEE Trans. on Smart Grid*, vol. 15, no. 1, pp. 886–898, 2023.

[7] S. Oshnoei *et al.*, "Model-free predictive frequency control under sensor and actuator fdi attacks," *IEEE Trans. on Circuits and Systems II: Express Briefs*, vol. 71, no. 4, pp. 2434–2438, 2023.

[8] A. Selim *et al.*, "Large language model for smart inverter cyber-attack detection via textual analysis of volt/var commands," *IEEE Trans. on Smart Grid*, 2024.

[9] H. Zhang *et al.*, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29 641–29 659, 2021.

[10] Y. Pei *et al.*, "Visibility-enhanced model-free deep reinforcement learning algorithm for voltage control in realistic distribution systems using smart inverters," *Applied Energy*, vol. 372, p. 123758, 2024.

[11] O. Khan *et al.*, "Impact of electric vehicles botnets on the power grid," in *2019 IEEE Electrical Power and Energy Conference (EPEC)*. IEEE, 2019, pp. 1–5.

[12] C. Alcaraz *et al.*, "Ocpp protocol: Security threats and challenges," *IEEE Trans. on Smart Grid*, vol. 8, no. 5, pp. 2452–2459, 2017.

[13] S. Maleki *et al.*, "The impact of load altering attacks on distribution systems with zip loads," in *2024 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2024, pp. 1–5.

[14] I. Sengor *et al.*, "Optimal energy management of ev parking lots under peak load reduction based dr programs considering uncertainty," *IEEE Trans. on Sustainable Energy*, vol. 10, no. 3, pp. 1034–1043, 2018.

[15] A. Koufakis *et al.*, "Offline and online electric vehicle charging scheduling with v2v energy transfer," *IEEE Trans. on Intelligent Transportation Systems*, vol. 21, no. 5, pp. 2128–2138, 2019.

[16] M. Baran *et al.*, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Trans. on Power delivery*, vol. 4, no. 2, pp. 1401–1407, 2002.