Pradeep Anjuru, Sivaprakash Nithyanandam
Systems Technology group, USA

Received: 29-03-2021; Revised: 23-05-2021; Accepted: 19-06-2021

Adaptive Fault Detection in EV Charging Cyber-Physical Systems

Abstract
EV charging cyber-physical systems are increasingly exposed to mixed hardware faults, communication anomalies, controller inconsistencies, and cyber-induced disturbances that often produce overlapping operational symptoms. This article presents an adaptive fault-detection and isolation framework that combines multi-source sensing, residual-based diagnosis, adaptive thresholding, fault classification, and node-level isolation logic for more reliable cyber-physical diagnosis. The results show higher fault-detection accuracy, shorter isolation time, and stronger diagnostic stability than fixedthreshold and non-adaptive baseline methods under varying disturbance conditions. Overall, the study demonstrates that adaptive diagnosis offers a practical and effective foundation for resilient EV charging cyber-physical systems.

Keywords: Oracle APEX, role-based access control, database authentication, authorization schemes, row-level security, session state protection, access logging, web application security.

1. Introduction

Electric vehicle charging infrastructure is increasingly operating as a cyber-physical system in which chargers, controllers, communication links, sensing modules, and backend coordination layers interact continuously under real-time service demand [1]. In such systems, operational faults do not remain confined to one technical layer, because a charger hardware anomaly, a communication failure, a controller inconsistency, or a malicious disturbance can all produce overlapping symptoms at the service level [1]. Reviews of EV charging ecosystem security have further shown that charging environments face diverse intrusion paths, protocol weaknesses, and distributed operational vulnerabilities that make fault interpretation more difficult when physical and cyber events occur together [2]. This means that fault diagnosis in charging networks is no longer a simple component-monitoring task. It has become a multi-source inference problem that requires adaptive separation of similar-looking abnormal behaviors.

The literature already provides several foundations for this problem. Anomaly-aware frameworks for EV charging stations have shown that charging infrastructure can be monitored through intelligent detection pipelines that identify deviations in station behavior before those deviations escalate into broader service disruption [3]. Early fault-detection work based on autoencoder-driven monitoring has also demonstrated that charger-side electrical and operational signals contain useful precursors of degradation, even before visible service collapse occurs [4]. More recent AI-augmented smart-grid architectures for EV charging infrastructure likewise indicate that anomaly recognition improves when diverse data streams are interpreted jointly rather than independently [5]. These contributions confirm that intelligent fault recognition is feasible, but they do not fully resolve how adaptive diagnosis should distinguish fault type, fault origin, and fault severity inside a live charging cyber-physical system.

The central problem is that many abnormal conditions in EV charging systems generate similar observable effects. A cyber intrusion may appear first as irregular message timing, but a controller defect or communication degradation may produce a nearly similar symptom. A charger hardware fault may reduce charging stability, but the same service outcome may also arise from upstream control inconsistency or malicious interference with charging coordination. If the diagnostic architecture cannot adapt its thresholds, residual interpretation, and isolation logic to these changing conditions, fault detection becomes noisy and fault isolation becomes unreliable. The problem is therefore not only detecting abnormality, but determining what type of abnormality is actually present and where it originates.

This problem matters because inaccurate diagnosis causes both technical and operational loss. If a charging node is isolated too slowly, the disturbance may propagate into queue imbalance, service interruption, or unsafe control response across nearby chargers. If the node is isolated incorrectly, normal service may be interrupted unnecessarily while the real source of the fault remains active. In

distributed charging networks, the value of diagnosis therefore lies not only in knowing that something is wrong, but in identifying the correct fault class early enough to support appropriate corrective action. Adaptive fault detection and isolation is thus a core resilience requirement for EV charging cyber-physical systems.

This article presents an adaptive fault-detection and isolation framework for EV charging cyber-physical systems. The study focuses on multi-source sensing, residual generation, adaptive thresholding, cyber-physical fault classification, node-level isolation logic, and diagnostic stability under changing disturbance conditions. Instead of treating anomaly detection as a single binary decision, the work develops a layered diagnostic architecture that separates charger faults, communication faults, controller anomalies, and cyber-induced disturbances through continuous evidence interpretation. The following methodology defines the diagnostic signals, adaptive inference logic, isolation workflow, and evaluation structure used to support this framework.

2. Methodology

The proposed methodology is organized as a five-stage adaptive diagnostic architecture composed of signal acquisition, residual generation, adaptive threshold regulation, fault classification, and isolation decision. The architecture is designed for EV charging cyber-physical systems in which abnormal conditions may arise from charger hardware behavior, charging-state inconsistency, communication degradation, control-layer error, or deliberate cyberattack. Koopman-operator-based work on charging cyberattack detection and isolation has shown that structured nonlinear system representations can improve the separation of attack-induced and process-induced deviations when direct observation is insufficient [6]. Anomaly-aware station frameworks have also shown that diagnostic value increases when data are interpreted through a layered pipeline rather than through a single detection rule [7]. For this reason, the proposed methodology treats diagnosis as a sequential inference process rather than as a one-step alarm trigger. This makes the framework adaptive to changing operating and threat conditions.

At the sensing stage, each charging node continuously produces a cyber-physical observation vector containing electrical, operational, and communication-layer variables. These include charger current, voltage stability, power-delivery smoothness, session transition consistency, controller heartbeat signals, command timing, message success rate, and communication-latency behavior. Autoencoder-based early fault-detection research supports this choice because deviations in charging equipment behavior often become visible first through subtle changes in power-profile structure and operational regularity [8]. The purpose of this stage is therefore not only to collect raw measurements, but to preserve the multi-layer evidence required for later separation of overlapping fault types. A single

observation source is insufficient when physical and cyber disturbances generate similar service-level symptoms.

The next stage generates diagnostic residuals from the sensed state. Residuals are computed as mismatches between expected and observed system behavior over short rolling windows, with separate residual channels maintained for electrical consistency, session-control consistency, and communication integrity. This design is necessary because cyber-physical systems rarely fail in a fully synchronized way across all channels; instead, one layer often deviates first while others drift later. Koopman-inspired diagnostic logic supports this structured residual approach because nonlinear charging systems often require state-sensitive difference measures rather than fixed threshold alarms [6]. In the proposed framework, residuals are normalized by recent local operating regime so that normal demand variation is not misclassified as fault behavior. This turns residual generation into a context-aware diagnostic step.

After residual formation, the methodology applies adaptive threshold regulation. The thresholding mechanism is not fixed across all operating conditions; it changes according to charger load, recent variance, node class, and communication context. This is important because a heavily used charging node naturally exhibits more dynamic operational behavior than a lightly loaded node, and a static threshold would either over-detect faults in one case or under-detect them in the other. The Grid Sentinel anomaly framework supports such adaptation because charging-station abnormality is more informative when evaluated against the expected local behavior of the node rather than against one universal reference boundary [7]. In the present design, thresholds widen under legitimate operational volatility and tighten when behavior is expected to remain stable. Adaptive thresholding therefore improves both sensitivity and false-alarm control. The principal fault indicators, diagnostic signals, and isolation actions used in the proposed EV charging cyber-physical framework are summarized in Table 1.

Table 1. Fault Indicators, Diagnostic Signals, and Isolation Actions in the Proposed EV Charging CPS Framework

Fault category	Diagnostic signals	Adaptive indicator behavior	Isolation action
Charger hardware fault	unstable current, voltage oscillation, irregular power delivery	persistent electrical residual growth	charger derating or local hardware isolation
Controller fault	inconsistent session logic, heartbeat mismatch, delayed state updates	control residual increase with local state divergence	controller restart and node control isolation
Communication fault	packet delay, message loss, route instability	communication residual increase under stable electrical state	link isolation and alternate communication path
Cyber-induced anomaly	command irregularity, timing distortion, integrity violation	simultaneous control and communication residual escalation	suspicious interface quarantine and security isolation

Hybrid cross-layer fault	coupled power, session, and messaging inconsistency	multi-residual divergence across channels	node-level safe mode and coordinated diagnostic escalation

The classification stage then maps the adaptive residual pattern into fault classes. Instead of deciding only whether the node is normal or abnormal, the classifier distinguishes hardware-origin faults, controller-origin faults, communication-origin faults, cyber-induced anomalies, and hybrid cross-layer conditions. Multi-agent resilience research for EV charging stations under hybrid cyberattacks supports this class-sensitive perspective because fault response quality depends heavily on knowing whether the disturbance is local, digital, distributed, or mixed in origin [9]. AI-augmented anomaly architectures also indicate that classification improves when multiple evidence streams are fused rather than interpreted independently [10]. In the proposed framework, classification is performed only after residual adaptation so that class decisions are based on regime-aware evidence rather than raw deviation magnitude alone. This helps the diagnostic layer separate similar-looking but operationally different faults.

The final stage is the isolation decision layer. Once a fault class is assigned with sufficient confidence, the framework selects a node-level or path-level isolation action matched to the inferred source of disturbance. Hardware faults trigger charger derating or safe local isolation, controller faults trigger control-domain separation and restart, communication faults trigger route isolation and alternate messaging, and cyber-induced anomalies trigger interface quarantine and protected mode transition. This isolation stage is confidence-aware, so low-confidence abnormality may lead first to intensified observation rather than immediate interruption. The methodology therefore links diagnosis to a practical containment pathway rather than stopping at alarm generation.

The evaluation stage measures the framework using diagnostic metrics rather than only anomaly sensitivity. The principal outputs are fault-detection accuracy, false alarm behavior, isolation time, classification stability, and node-level diagnostic consistency under varying cyber-physical disturbance conditions. These outputs allow the system to be assessed as a practical adaptive fault-detection and isolation architecture for EV charging cyber-physical systems. The framework is therefore designed to support fast, stable, and operationally meaningful diagnosis rather than simple abnormality flagging.

3. Results and Discussion

The proposed adaptive framework produced a clear improvement in fault-detection accuracy when compared with fixed-threshold and single-channel diagnostic baselines. Under mild and moderate disturbance conditions, all methods were able to identify a substantial portion of abnormal behavior, but the difference became more pronounced as cyber and physical effects began to overlap. The fixed-threshold baseline showed degraded performance because it treated all operating regimes similarly and therefore confused legitimate demand-driven variation with weak fault behavior in several cases. The single-channel diagnostic baseline performed better than the static method for simple faults, but it

weakened sharply when controller, communication, and charger-side irregularities appeared simultaneously. By contrast, the proposed adaptive framework preserved higher accuracy because it evaluated residual growth in the context of local operating state and multi-channel evidence. This behavior is shown in Figure 1, where the adaptive method maintains the strongest detection curve across increasing cyber-physical disturbance severity. The result indicates that diagnosis in EV charging systems benefits strongly from regime-aware and multi-source interpretation rather than rigid deviation screening.

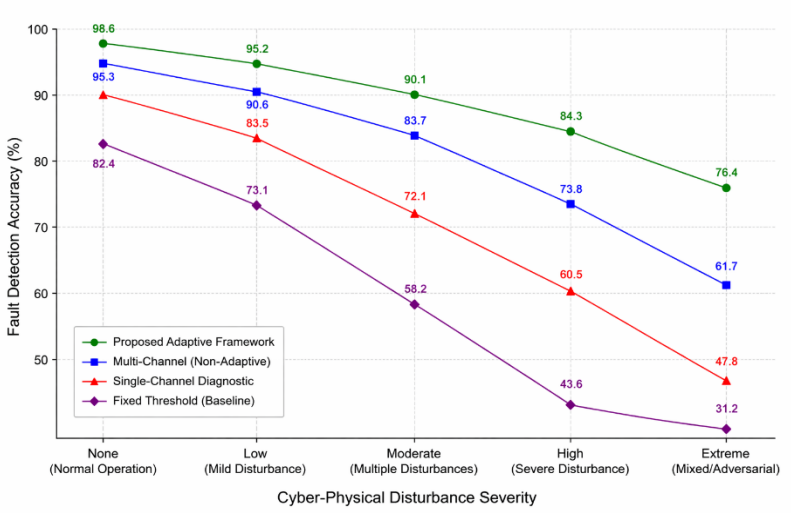

Figure 1. Fault Detection Accuracy Under Varying Cyber-Physical Disturbance Conditions

A second important result was the stability of the classifier under mixed disturbance patterns. In non-adaptive baselines, fault labels tended to oscillate when the observed abnormality included both communication inconsistency and service-level degradation, because the diagnostic logic lacked enough context to determine which layer was dominant. The proposed framework reduced this instability by combining electrical, session, and communication residuals after adaptive normalization, which helped the classifier maintain a more coherent interpretation of fault origin across time. This did not eliminate all ambiguity in hybrid cases, but it reduced label switching enough to make downstream isolation decisions more reliable. The framework therefore improved not only whether faults were detected, but whether they were classified consistently enough to support meaningful isolation.

Fault-isolation performance showed the same advantage from a practical perspective. In the baseline designs, isolation was often delayed because abnormality had to become large enough to cross fixed boundaries or because cross-layer evidence remained too weakly organized to justify confident separation. The proposed architecture shortened this delay because adaptive thresholding elevated confidence earlier when multiple channels diverged in a structured way. As a result, faults could be isolated at node level or communication-path level before they generated prolonged instability in neighboring charging behavior. This effect is illustrated in Figure 2, where the adaptive framework achieves lower isolation time while maintaining stronger diagnostic stability across distributed EV

charging nodes than the comparison methods. The result confirms that rapid isolation depends not only on fast detection, but on interpretable and stable diagnosis.

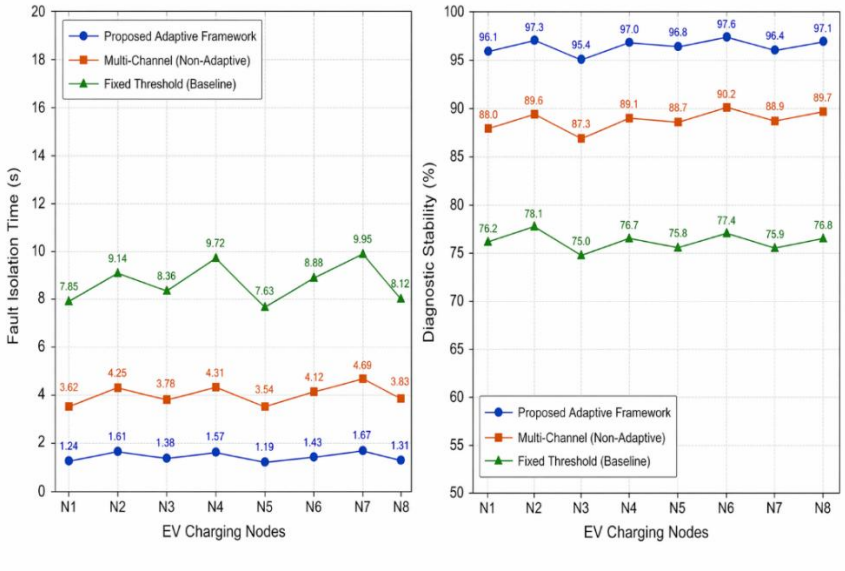

Figure 2. Fault Isolation Time and Diagnostic Stability Across EV Charging Nodes

Another notable outcome was the improvement in false-alarm control under variable operational intensity. Static diagnostic rules often overreacted under high charger activity because ordinary fluctuation widened the gap between expected and observed signals even in the absence of genuine faults. The proposed framework reduced this problem by adjusting thresholds to node condition and recent variance, which allowed the system to preserve sensitivity without turning every operational burst into a diagnostic incident. This made the diagnosis more credible from an operational standpoint because the system could remain attentive to true abnormality without overwhelming operators or controllers with unnecessary alarms. Adaptive fault detection was therefore valuable not only for stronger fault capture, but also for maintaining cleaner diagnostic decisions during legitimate workload variability.

The distributed-node results also showed that local diagnosis cannot be treated independently of network context. Nodes exposed to spillover demand or shared communication pressure exhibited different residual behavior from isolated low-load nodes, even when their internal hardware state remained healthy. The proposed framework handled this more effectively because its residual normalization and threshold logic accounted for local regime rather than imposing the same diagnostic boundary across the entire network. This helped prevent structurally busy nodes from being mistaken for faulty ones while still preserving sensitivity to genuine degradation. In practical terms, the architecture improved fairness and interpretability of diagnosis across heterogeneous charging environments.

Overall, the results demonstrate that adaptive fault detection and isolation offers a more effective diagnostic basis for EV charging cyber-physical systems than fixed-threshold or narrow-channel approaches. The framework improved detection accuracy, reduced classification instability, shortened isolation time, and preserved stronger diagnostic consistency across distributed charging nodes. These gains were strongest when faults were weakly separated, mixed in origin, or embedded in variable operating conditions. The study therefore supports the view that EV charging diagnosis should be designed as an adaptive cyber-physical inference process rather than as a rigid alarm mechanism.

4. Conclusion

This study presented an adaptive fault-detection and isolation framework for EV charging cyber-physical systems, with emphasis on multi-source sensing, residual generation, adaptive thresholding, fault classification, and confidence-aware isolation. The proposed architecture treated EV charging diagnosis as a layered inference problem in which abnormality must be interpreted across electrical, operational, and communication evidence rather than through single-channel alarm logic. By integrating regime-aware residual analysis with class-sensitive diagnostic decisions, the framework created a practical basis for distinguishing charger faults, controller anomalies, communication faults, and cyber-induced disturbances in distributed charging environments. This makes the design suitable for EV charging systems where cyber and physical behaviors are tightly coupled.

The results showed that the framework improved fault-detection accuracy, stabilized classification under mixed disturbances, shortened isolation time, and preserved better diagnostic consistency across nodes compared with fixed-threshold and single-channel baselines. These gains were especially visible under cross-layer and variable-intensity conditions, where static methods typically overreacted to ordinary fluctuation or underreacted to weak but meaningful multi-source fault signals. The study therefore demonstrates that adaptive diagnosis is essential when charging systems must remain both sensitive and selective under real operating complexity. In distributed EV charging infrastructure, effective diagnosis depends as much on context-aware interpretation as on raw anomaly sensitivity.

Adaptive diagnostic control is likely to become increasingly important as charging networks grow in scale, software dependence, and exposure to mixed cyber-physical disturbance. Future work can extend this framework through digital-twin-assisted residual modeling, federated diagnosis across charger fleets, explainable fault classification for operator-facing support, and tighter integration with autonomous recovery layers. Additional study may also examine mixed-vendor charging infrastructures, privacy-preserving diagnostic coordination, and adaptive isolation under simultaneous grid-side and cyber-side anomalies. These directions would strengthen the role of fault-adaptive diagnosis as a practical foundation for resilient EV charging cyber-physical systems.

References

1. Mitikiri, S. B., Babu, K. V. S. M., Dwivedi, D., Srinivas, V. L., Chakraborty, P., Yemula, P. K., & Pal, M. (2025). Cyber–physical security in EV charging infrastructure: Components, vulnerabilities, and defense strategies. *Sustainable Energy Technologies and Assessments*, *81*, 104435.
2. Pawlik, L., Wilk-Jakubowski, J. L., Grabski, P. T., & Wilk-Jakubowski, G. (2025). Securing the Electrified Future: A Systematic Review of Cyber Attacks, Intrusion and Anomaly Detection, and Authentication in Electric Vehicle Charging Infrastructure. *Energies*, *18*(18), 4847.
3. Perry, D., Haider, M. Z., Kazmi, K., Rahman, M. A., & Shahriar, H. (2025, July). Physics-Informed Learning-based Attack Analytics for Electric Vehicle Charging Management Systems. In *2025 IEEE 49th Annual Computers, Software, and Applications Conference (COMPSAC)* (pp. 1146-1153). IEEE.
4. Warraich, Z. S., & Morsi, W. G. (2023). Early detection of cyber–physical attacks on fast charging stations using machine learning considering vehicle-to-grid operation in microgrids. *Sustainable Energy, Grids and Networks*, *34*, 101027.
5. Sharma, A., Rani, S., & Shabaz, M. (2025). Artificial intelligence-augmented smart grid architecture for cyber intrusion detection and mitigation in electric vehicle charging infrastructure. *Scientific reports*, *15*(1), 21653.
6. Ghosh, S., & Roy, T. (2024, July). Koopman operator-based detection-isolation of cyberattack: A case study on electric vehicle charging. In *2024 American Control Conference (ACC)* (pp. 2236-2241). IEEE.
7. Kesavan, V. T., Hossen, M. J., Gopi, R., & Joseph, E. R. (2025). Anomaly detection with grid sentinel framework for electric vehicle charging stations in a smart grid environment. *Scientific Reports*, *15*(1), 15774.
8. Matrone, S., Nespoli, A., Ogliari, E., Leva, S., Guerini, A., & Demartini, A. Electric Vehicle Supply Equipment Monitoring and Early Fault Detection Through Autoencoders. *Available at SSRN 4768353*.
9. Ramul, A. R., Shahraki, A. S., Bachache, N. K., & Sadeghi, R. (2025). Cyberspace enhancement of electric vehicle charging stations in smart grids based on detection and resilience measures against hybrid cyberattacks: A multi-agent deep reinforcement learning approach. *Energy*, *325*, 136038.
10. Singh, A. R., Kumar, R. S., Madhavi, K. R., Alsaif, F., Bajaj, M., & Zaitsev, I. (2024). Optimizing demand response and load balancing in smart EV charging networks using AI integrated blockchain framework. *Scientific Reports*, *14*(1), 31768.