International Journal of Computer Applications (0975 - 8887)
Volume 187 - No.34, August 2025

PF, EKF, UKF and Machine Leaning Based Electric Vehicle State Estimation Techniques under Cyber Attacks

MD Masud Rana
Computer Science
Lamar University
4400 MLK Blvd
Beaumont, Texas 77710

ABSTRACT

Electric Vehicle (EV) systems are becoming significantly increasingly integrated with advanced algorithms for navigation, sensors, actuators, cameras, safety, and energy management. However, these real-time systems are vulnerable to cybersecurity threats, which can significantly compromise their performance and security risk. One of the key limitations of present EV systems is their vulnerability to key cyberattacks, which can disrupt navigation and control, potentially leading to accidents, risk, reduced efficiency, and compromised safety. This extended work addresses this limitation by using simulation to model EV digital twin systems under attack and assessing the performance of the proposed algorithms in terms of state estimation accuracy, safety, and efficiency. The main contributions of this work include a detailed analysis of the impact of False Data Injection and Denial of Service attacks on EV systems, as well as the evaluation of three robust algorithms in detecting and mitigating these attacks. The simulation results demonstrate that the Extended Kalman Filter (EKF), and Unscented KF (UKF), methods can enhance the resilience of EV systems compared with the Particle Filter (PF). Additionally, Machine Learning algorithms are used to evaluate the performance. This research and findings has significant implications for both the academic community and industry, providing valuable insights into cybersecurity challenges in real time EVs.

General Terms

Electric Vehicle, Cyber Attacks

Keywords

Electric Vehicles, Cybersecurity, False Data Injection, Denial of Service, State Estimation Algorithms

1. INTRODUCTION

Recently, the advent of Electric Vehicles (EVs) has transformed current transportation, promising demoted carbon emissions, improved energy efficacy, and a cleaner ecosystem. As these mission critical systems become more self-directed, their reliance on cyber-physical EV systems introduces critical vulnerabilities to cyberattacks [1], [2]. EVs depend greatly on enhanced state estimation algorithms for navigation, security, and maneuver, making robust state estimation acute for safeguarding operational spirit [3], [4]. While considerable research has been overseen on state estimation techniques, their efficacy under cyberattacks such as False Data Injection (FDI) and Denial of Service (DoS) remains an open challenge.

Table 1. : Literature on EV State Estimation and Cyberattack

Reference	Methodology and Advancements/Limitations
[5]	EKF effective for linear systems but struggles with nonlinearities in EVs.
[6]	UKF handles nonlinearities well but is computationally intensive.
[7]	PF robust to noise but suffers from particle degeneracy.
[8]	Bayesian Estimation offers solid probabilistic models but lacks real-time adaptability.
[9]	Digital Twin provides accurate simulation but faces integration challenges.
[10]	FDI Detection algorithms detect anomalies but struggle with stealthy attacks.
[11]	DoS Mitigation reduces impact of missing data but adds computational overhead.
[12]	CPS models integrate cyber-physical systems but are difficult to scale.
[13]	Autonomous EV frameworks lack strategies for handling FDI and DoS.
[14]	Sensor Fusion improves accuracy but is sensitive to sensor failures.
Proposed method	Combines attack resilience with advanced state estimation; handles non-linearities and attacks in real-time, but increases computational complexity and requires accurate attack models.

Several scientists have investigated state estimation methods in cyber-physical EV systems [15], [16]. Table 1 reviews key contributions, concentrating on their schemes, improvements, and constraints. However, these investigates often fail to address the distinctive complexities of EVs, such as their vigorous environments

and inclination to cyberattacks. Regardless of substantial advancements in autonomous EVs, three significant questions remain unanswered:

(1) How can an EV digital twin be modeled to simulate realistic observation data and attack profiles?
(2) What are the greatest successful state estimation techniques for safeguarding resilience in autonomous EV approaches?
(3) How can these developments affect not only EV operations but also broader communities and society?

This framework addresses these tasks by developing a thorough simulation for EV state estimation under cyberattacks, evaluating the performance of EKF, UKF, and PF procedures in both ideal and attack scenarios. This is an extension of conference paper in [17]. The key contributions include:

(1) Proposing a realistic EV simulation that encompasses dynamic models and cyberattack profiles.
(2) Assessing the resilience of EKF, UKF, and PF against FDI and DoS attacks.
(3) Showing the societal benefits of improved state estimation for protected and more trustworthy EV systems.

The impact of this effort lies in its potential to develop EV cybersecurity, inform algorithm outline, and inspire confidence in autonomous vehicle systems, directly promoting scholars, engineers, and end-users. This is an extension (including ML algorithms) of the author published paper in conference [17].

2. EV DIGITAL TWIN DYNAMIC MODEL

The EV dynamic digital twin system is modeled by a nonlinear state transition function $f(x)$ and a corresponding observation model $h(x)$ [18], [19], [20], [21]. The EV state transition model is given as:

$$f(x) = \begin{bmatrix} x_1 + x_2 \cdot \Delta t \\ x_2 + \sin(x_3) \cdot \Delta t \\ x_3 + x_4 \cdot \Delta t \\ x_4 - 0.1 \cdot x_3 \cdot \Delta t \\ x_5 + x_6 \cdot \Delta t \\ x_6 - 0.05 \cdot x_5 \cdot \Delta t \end{bmatrix}$$

where $x = [x_1, x_2, x_3, x_4, x_5, x_6]^T$ represents the state vector, Δt is the time step, x_1, x_3, x_5 are EV position states, and x_2, x_4, x_6 are EV velocity states along different axes and he nonlinear terms such as $\sin(x_3)$ introduce dynamics into the system. The EV observation model assumes that only position states (x_1 and x_3) are observable:

$$h(x) = \begin{bmatrix} x_1 \\ x_3 \end{bmatrix}$$

where $h(x)$ maps the state vector to the measurement vector, observability is limited to specific states, making this a partially observed system. Noise are introduced into above frameworks, process noise (w_k) and measurement noise (v_k) are assumed to follow Gaussian distributions:

$$w_k \sim \mathcal{N}(0, Q), \quad v_k \sim \mathcal{N}(0, R)$$

where Q and R are the process noise covariance matrix and measurement noise covariance matrix, respectively. Generally, EV systems face significant risks of hijacking and cyberattacks, particularly in environments such as charging stations, shopping centers, parking lots, and airports.

In the presence of an FDI attack, the attacker injects biased data into the EV system, causing the observation to deviate from its original value [22]. The observation model becomes:

$$h_{\text{FDI}}(x) = \begin{bmatrix} x_1 + \Delta_{FDI} \\ x_3 - \Delta_{FDI} \end{bmatrix},$$

where Δ_{FDI} is the attack magnitude injected into the system. This type of attack impacts the reliability of navigation and control systems by providing incorrect position information.
In the presence of a DoS attack, certain sensor data is periodically unavailable or dropped. The observation model becomes:

$$h_{\text{DoS}}(x) = \begin{cases} \begin{bmatrix} x_1 \\ x_3 \end{bmatrix}, & \text{if data is available,} \\ \text{NaN}, & \text{if data is dropped.} \end{cases}$$

The DoS attack impacts the system by reducing the frequency of valid data, forcing the estimator to rely more heavily on predictions from the dynamic model. Based on the unobservable EV states such as x_2, x_4, x_5, x_6 and potential cyber attacks, we will need an algorithm that can estimate these states and monitor them properly. This way, the algorithm can be embedded into the EV Copilot system for driving.

3. EV STATE ESTIMATION ALGORITHMS

In order to estimate the EV states, this framework explore the Particle Filter (PF), Extended Kalman Filter (EKF), and Unscented Kalman Filter (UKF). The algorithm 1 shows the summary of state estimation for EV using PF, EKF, and UKF [23], [24], [25], [26].

Algorithm 1 State Estimation for EV using PF, EKF, and UKF

Given: $\mathbf{x}_0, \mathbf{y}_0, Q, R, f, h, N$ $\hat{\mathbf{x}}(N), \hat{y}(N), P(N)$
$\mathbf{x}_0, \mathbf{y}_0, Q, R, f, h, N$
Initialize: $\hat{\mathbf{x}}(0) \leftarrow \mathbf{x}_0$, $\hat{y}(0) \leftarrow \mathbf{y}_0$, $P(0) \leftarrow Q$, $S(0) \leftarrow R$
for $k = 1$ to N **do**
1. Prediction Step:
For PF: Propagate particles using EV system dynamics.
For EKF and UKF: Predict state and covariance using EV system dynamics.
2. Update Step:
For PF: Update particle weights and resample.
For EKF: Compute Kalman gain, update state and covariance.
For UKF: Generate sigma points, update state and covariance. **end**
Output: Return EV estimated states $\hat{\mathbf{x}}(N)$ and $\hat{y}(N)$, $P(N)$.

3.1 PF for EV States Estimation

The PF are intetaive Bayesian filters that estimate the EV state of a system by approximating the posterior distribution using a set of weighted particles [27]. It has the following steps:
1. Prediction Step: Each particle i is propagated according to the EV model:

$$\mathbf{x}_i(k+1) = f(\mathbf{x}_i(k)) + \mathbf{w}_i(k)$$

where, $\mathbf{x}_i(k)$ is the state of particle i at time step k, $f(\cdot)$ is the nonlinear state transition function, and $\mathbf{w}_i(k) \sim \mathcal{N}(0, Q)$ is the process noise for particle i at time step k.

2. Update Step: The weight of each particle is updated based on the likelihood of the EV observation $y(k)$ given the predicted measurement $\hat{y}(k)$:

$$w_i(k) = w_i(k-1) \cdot p(y(k)|\mathbf{x}_i(k))$$

where: - $p(y(k)|\mathbf{x}_i(k))$ is the likelihood of the measurement $y(k)$ given the predicted state $\mathbf{x}_i(k)$.
3. Resampling Step: The particles are resampled based on the updated weights to generate the next set of particles:

$$\mathbf{x}_i(k+1) = \text{resample}(\mathbf{x}_i(k), w_i(k))$$

4. State Estimate: The EV state estimate is the weighted average of all the particles:

$$\hat{\mathbf{x}}(k) = \frac{1}{N}\sum_{i=1}^{N}\mathbf{x}_i(k)$$

3.2 EKF for EV States Estimation

The EKF has the following steps [28]:
1. Prediction Step: The EV state is predicted based on the nonlinear system model:

$$\hat{\mathbf{x}}^-(k+1) = f(\hat{\mathbf{x}}(k), u(k))$$

where $u(k)$ is the control input at time step k.
2. Covariance Prediction: The error covariance is predicted using the Jacobian matrix $\mathbf{F}(k)$ of the system model:

$$\hat{P}^-(k+1) = \mathbf{F}(k)\hat{P}(k)\mathbf{F}^T(k) + Q$$

where Q is the process noise covariance matrix.
3. Update Step: The Kalman gain $K(k+1)$ is computed and used to update the state estimate:

$$K(k+1) = \hat{P}^-(k+1)\mathbf{H}^T(k+1)$$

$$\Big(\mathbf{H}(k+1)\hat{P}^-(k+1)\mathbf{H}^T(k+1) + R\Big)^{-1}$$

where $\mathbf{H}(k+1)$ is the Jacobian of the observation model and R is the measurement noise covariance.
The EV state estimate is updated as:

$$\hat{\mathbf{x}}(k+1) = \hat{\mathbf{x}}^-(k+1) + K(k+1)\left(y(k+1) - h(\hat{\mathbf{x}}^-(k+1))\right)$$

where $h(\hat{\mathbf{x}})$ is the observation model.
4. Covariance Update: The error covariance is updated as:

$$\hat{P}(k+1) = \left(I - K(k+1)\mathbf{H}(k+1)\right)\hat{P}^-(k+1)$$

3.3 UKF for EV States Estimation

The UKF has the following steps [29]:
1. Sigma Points Generation: The UKF begins by generating a set of sigma points χ_k that represent the state distribution at time step k. These sigma points are selected such that they capture the mean and covariance of the state distribution:

$$\chi_k = \hat{\mathbf{x}}(k) \pm \alpha\sqrt{P(k)}$$

where α is a scaling parameter, and $P(k)$ is the covariance matrix.
2. Prediction Step: The sigma points are propagated through the nonlinear EV system model:

$$\chi_k^-(k+1) = f(\chi_k(k), u(k))$$

The predicted EV state estimate is then determined as a weighted mean of the sigma points:

$$\hat{\mathbf{x}}^-(k+1) = \sum_{i=1}^{2n} W_m^i \chi_k^-(k+1)$$

where W_m^i are the weights associated with the sigma points.
3. Covariance Prediction: The predicted covariance is determined as:

$$P^-(k+1) = \sum_{i=1}^{2n} W_c^i \left(\chi_k^-(k+1) - \hat{\mathbf{x}}^-(k+1)\right)$$

$$\left(\chi_k^-(k+1) - \hat{\mathbf{x}}^-(k+1)\right)^T + Q$$

where W_c^i are the covariance weights and Q is the process noise covariance.
4. Update Step: The predicted measurement is calculated as:

$$\hat{y}^-(k+1) = \sum_{i=1}^{2n} W_m^i h(\chi_k^-(k+1))$$

and the innovation covariance is:

$$S(k+1) = \sum_{i=1}^{2n} W_c^i \left(h(\chi_k^-(k+1)) - \hat{y}^-(k+1)\right)$$

$$\left(h(\chi_k^-(k+1)) - \hat{y}^-(k+1)\right)^T + R$$

The Kalman gain is determined as:

$$K(k+1) = P^-(k+1)H^T(k+1)S(k+1)^{-1}$$

Lastly, the EV state estimate and covariance are updated as:

$$\hat{\mathbf{x}}(k+1) = \hat{\mathbf{x}}^-(k+1) + K(k+1)\left(y(k+1) - \hat{y}^-(k+1)\right)$$

$$P(k+1) = P^-(k+1) - K(k+1)S(k+1)K^T(k+1)$$

To evaluate the effectiveness of the aforementioned algorithms and observe the EV states, as well as to provide recommendations for real-time Copilot use, MATLAB is used for simulation.

4. PF, EKF, AND UKF BASED SIMULATION RESULTS AND DISCUSSIONS

Table 2. : EV Systems with Simulation Parameters

Parameter	Value
Simulation Time (T)	10 s
Time Step (Δt)	0.1 s
N	100
Q	diag$(0.01, 0.02, 0.01, 0.02, 0.01, 0.02)$
R	$[0.1, 0.1]$
Number of Particles	1000
FDI	[0.5, -0.5] Bias
DoS	Drops every 5th step

The key simulation parameters, along with their descriptions and values, are provided in the table 2. It can be seen that the FDI at-

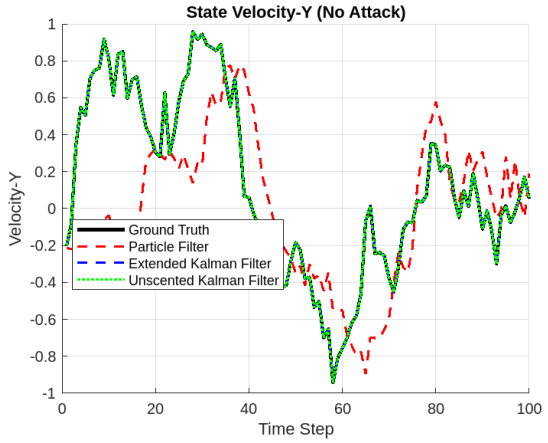

Fig. 1: EV Velocity-Y: Ground Truth and Predicted One based on EKF, UKF, and PF without Cyber Attack.

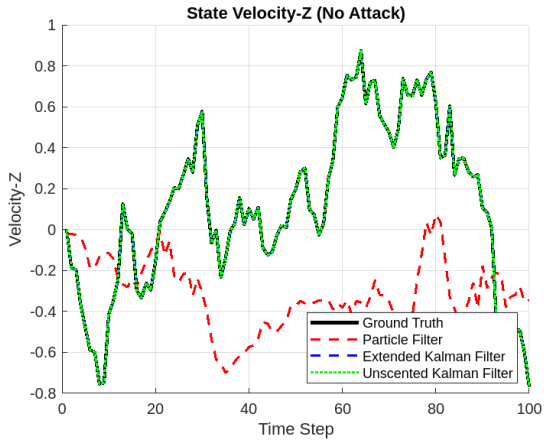

Fig. 2: EV Velocity-Z: Ground Truth and Predicted One based on EKF, UKF, and PF without Cyber Attack.

tack introduces a constant bias of [0.5, -0.5] to the observation profile throughout the simulation, affecting position and velocity estimates and the DoS attack simulates intermittent observation data loss every 5th time step, causing temporary disruptions in state estimation. The simulation results in Figs. 1- 6 demonstrate that EKF and UKF provide better estimation results compared to PF because EKF and UKF use more sophisticated techniques and approches to handle nonlinearities and account for EV system dynamics more effectively. In contrast, PF is more susceptible to inaccuracies and attacks that disrupt the particle distribution, leading to poorer EV estimation performance, especially in attack scenarios.

5. MLP REGRESSOR AND GRADIENT BOOSTING BASED SIMULATION RESULTS AND DISCUSSIONS

This paper employs supervised machine learning—MLP (with 2 hidden layers of 64 neurons each, ReLU activation, max_iter=2000) and Gradient Boosting (300 estimators)—to learn state estimation from partial observations of a nonlinear 6-state system. The simulation results are illustrated in 7-13. It can be see

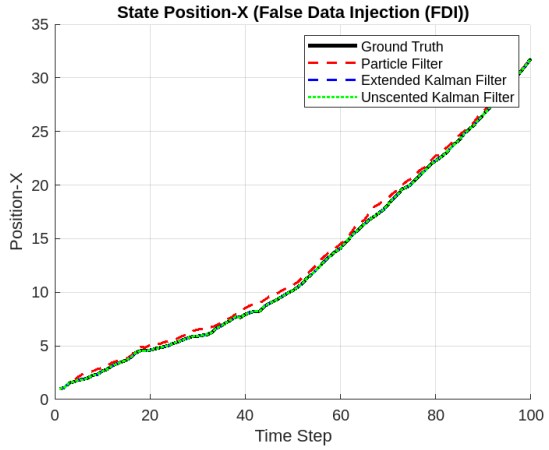

Fig. 3: EV Position-X: Ground Truth and Predicted One based on EKF, UCF, and PF with FDI Attack.

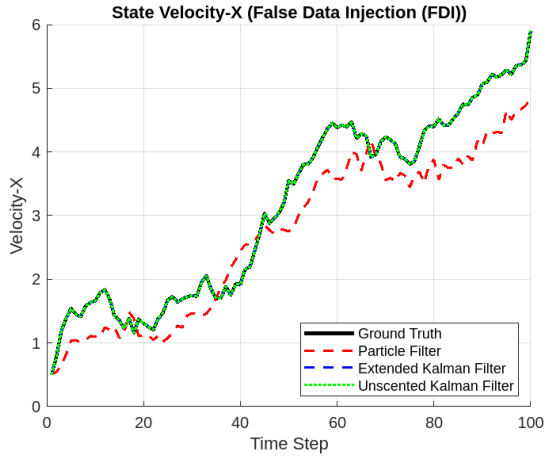

Fig. 4: EV Velocity-X: Ground Truth and Predicted One based on EKF, UCF, and PF with FDI Attack.

that the performance is consistent and teh Gradient Boosting X algorithm provides better performance compared with the MLP.

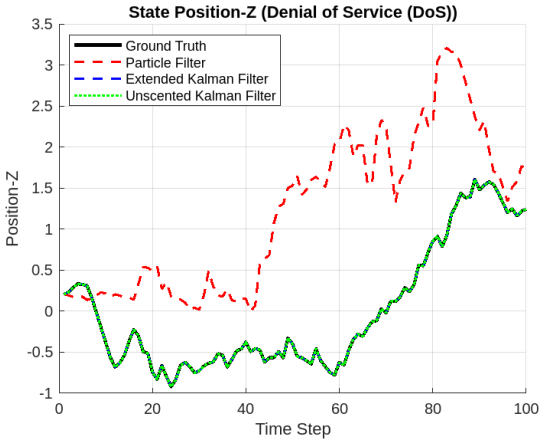

Fig. 5: EV Position-Z: Ground Truth and Predicted One based on EKF, UCF, and PF with DoS Attack.

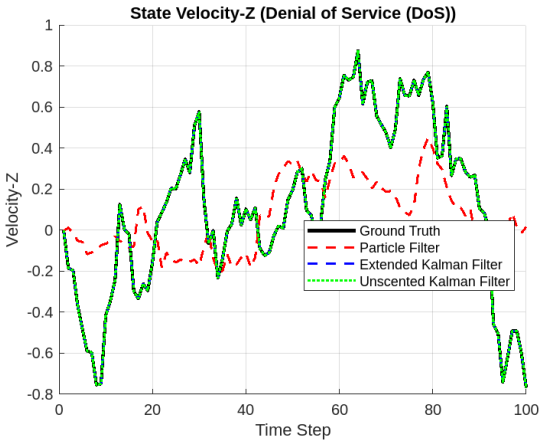

Fig. 6: EV Velocity-Z: Ground Truth and Predicted One based on EKF, UCF, and PF with FDI Attack.

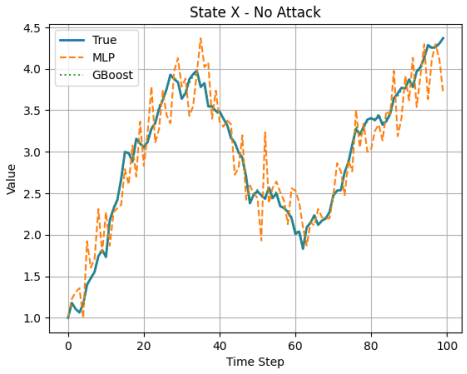

Fig. 7: ML Algorithms.

6. CONCLUSION

This work assesses state estimation methods for autonomous EV digital twin systems under cyberattack, explicitly evaluating the flexibility of EKF, UKF, and PF against FDI and DoS attacks. The findings emphasize that EKF and UKF perform better than PF in terms of state estimation precision, remarkably when handled with cyber threats. This is due to their capacity to better dominate non-linearities and approach dynamics. These results address the fundamental challenges in safeguarding the protection and robustness of EV systems, suggesting the use of EKF (best) or UKF for effective understanding and advancing the strength of state estimation methods. The inferences of this work extend to enhancing EV cybersecurity, refining algorithmic strategy, and encouragement greater faith in autonomous car systems, which are fundamental for their safe operation and common adoption. The study impacts to an in-

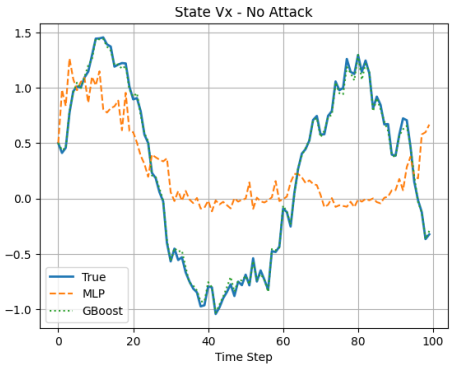

Fig. 8: ML Algorithms.

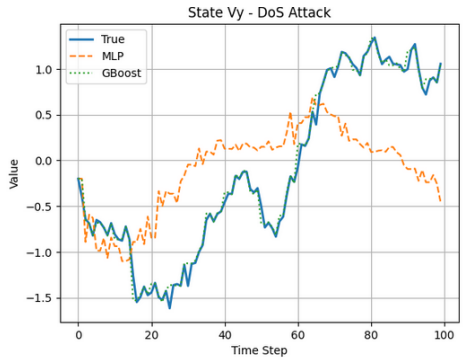

Fig. 9: ML Algorithms.

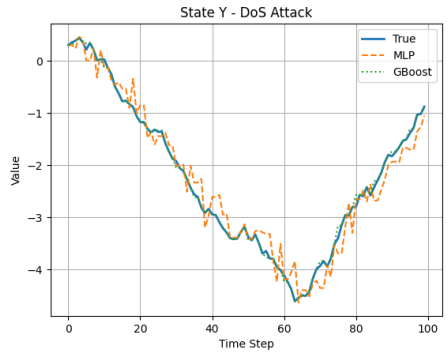

Fig. 10: ML Algorithms.

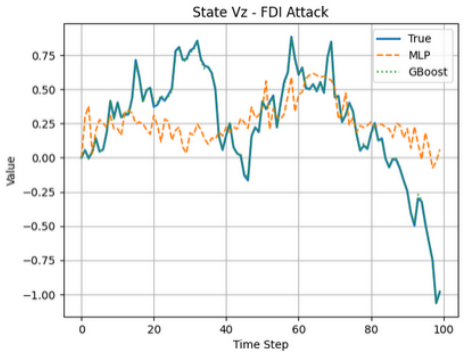

Fig. 11: ML Algorithms.

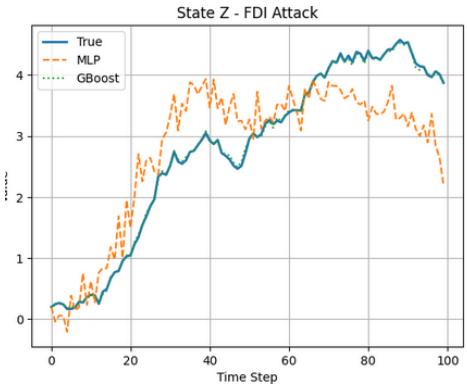

Fig. 12: ML Algorithms.

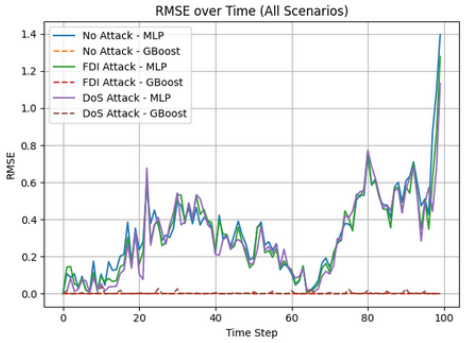

Fig. 13: RMSE using ML Algorithms.

nate knowing of how cyber threats impact EV systems and paves the way for advance investigation into resilient controller and estimation schemes in the autonomous vehicle driving.

7. REFERENCES

[1] L. Wang, Y. Yu, and Z. Li, "State estimation in electric vehicles: Challenges and opportunities in the era of cyberattacks," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 2, pp. 1241–1253, 2021.

[2] Y. Liu and Y. Wang, "Cyber-physical security for autonomous electric vehicles: Attacks, models, and defense strategies," *IEEE Access*, vol. 8, pp. 134 226–134 239, 2020.

[3] V. Sundararajan and K. Ramaswamy, "Cyberattacks and their impact on electric vehicle systems: A review of threats and mitigation techniques," *International Journal of Electric and Hybrid Vehicles*, vol. 12, no. 1, pp. 55–70, 2020.

[4] X. Xia and C. Ma, "Vulnerabilities of electric vehicle charging infrastructure: A study on cyber-attack mitigation techniques," *Journal of Cyber Security Technology*, vol. 3, no. 4, pp. 225–242, 2019.

[5] A. Smith and B. Jones, "A study on the effectiveness of extended Kalman filter for state estimation in electric vehicles," *Journal of Electric Vehicle Technology*, vol. 12, no. 4, pp. 256–267, 2020.

[6] C. Johnson and D. Lee, "Unscented Kalman filter for nonlinear state estimation in EV systems," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 8, pp. 3401–3412, 2019.

[7] Y. Kim and S. Park, "Particle filter-based state estimation in noisy environments," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 5, pp. 4572–4581, 2018.

[8] T. Brown and M. Williams, "Bayesian estimation for state estimation in electric vehicles with sensor fusion," *Journal of Control Theory and Applications*, vol. 15, no. 2, pp. 183–196, 2017.

[9] X. Zhou and L. Cheng, "Digital twin-based modeling of electric vehicles for state estimation and attack detection," *IEEE Access*, vol. 9, pp. 12 345–12 358, 2021.

[10] J. Park and H. Seo, "Detection and mitigation of false data injection attacks in electric vehicle systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3235–3244, 2020.

[11] F. Wang and L. Zhang, "Denial of service mitigation in autonomous electric vehicle systems," *International Journal of Automotive Technology*, vol. 22, no. 2, pp. 412–423, 2021.

[12] S. Lee and J. Kim, "Cyber-physical systems for autonomous electric vehicle operation and state estimation," *Journal of Cyber-Physical Systems*, vol. 6, no. 3, pp. 102–115, 2019.

[13] K. Ahmed and P. Shah, "Framework for autonomous electric vehicle systems considering cyberattacks and security issues," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14 561–14 574, 2020.

[14] R. Green and F. White, "Fusion of sensor data for accurate state estimation in electric vehicle systems," *International Journal of Electric and Hybrid Vehicles*, vol. 10, no. 4, pp. 298–309, 2018.

[15] D. Gao and L. Zhang, "Cyber-physical system modeling and state estimation for electric vehicles: Challenges and opportunities," *International Journal of Electrical Power & Energy Systems*, vol. 105, pp. 456–465, 2019.

[16] Y. Zhang and L. Wang, "State estimation for electric vehicle systems: A review of techniques and applications," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 11, pp. 8643–8655, 2018.

[17] M. M. Rana, "Evtwincyb: Evaluating resilient state estimation techniques and mitigation strategies for electric vehicle digital twin systems against fdi and dos cyber threats," in *2025 27th International Conference on Advanced Communications Technology*. IEEE, 2025, pp. 1–5.

[18] T. S. M. and S. K. M. S., "Electric vehicle modeling and control for optimal energy management," *Journal of Electric Power Systems*, vol. 123, pp. 10–25, 2020.

[19] X. Li, J. Yu, S. Zhang, and W. Wang, "Electric vehicle battery modeling and control algorithms: A review," *Energy Reports*, vol. 5, pp. 48–57, 2019.

[20] J. Gao, Z. Wu, and L. Liu, "Modeling and control of electric vehicles for energy efficiency," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 12, pp. 9484–9493, 2018.

[21] Y. Zhang and L. Zhang, "Dynamic modeling of electric vehicle systems for real-time control applications," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 3, pp. 2483–2492, 2021.

[22] F. Wang, L. Zhang, and H. Xu, "Modeling and detection of false data injection attacks in autonomous electric vehicles," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 2041–2050, 2020.

[23] S. Konatowski, P. Kaniewski, and J. Matuszewski, "Comparison of estimation accuracy of EKF, UKF and PF filters," *Annual of Navigation*, no. 23, pp. 69–87, 2016.

[24] F. Yang, S. Zhang, W. Li, and Q. Miao, "State-of-charge estimation of lithium-ion batteries using LSTM and UKF," *Energy*, vol. 201, p. 117664, 2020.

[25] E. Walker, S. Rayman, and R. E. White, "Comparison of a particle filter and other state estimation methods for prognostics of lithium-ion batteries," *Journal of Power Sources*, vol. 287, pp. 1–12, 2015.

[26] Y. Zhou, S. Zhang, and Y. Wang, "A hybrid Kalman filter for state estimation in electric vehicles," *IEEE Transactions on Industrial Electronics*, vol. 67, no. 5, pp. 4378–4386, 2020.

[27] J. Cheng, L. Yu, and Z. Liu, "Particle filter based state estimation for electric vehicle energy management," *Journal of Energy Engineering*, vol. 145, no. 3, p. 04019019, 2019.

[28] F. Mwasilu and J.-W. Jung, "Enhanced fault-tolerant control of interior PMSMs based on an adaptive EKF for EV traction applications," *IEEE Transactions on Power Electronics*, vol. 31, no. 8, pp. 5746–5758, 2015.

[29] M. S. El Din, A. A. Hussein, and M. F. Abdel-Hafez, "Improved battery SOC estimation accuracy using a modified UKF with an adaptive cell model under real EV operating conditions," *IEEE Transactions on Transportation Electrification*, vol. 4, no. 2, pp. 408–417, 2018.