Integrating the Internet of Things to Protect Electric Vehicle Control Systems from Cyber Attacks

Baddu Naik Bhukya, *Member, IAENG*, V. Venkataiah, S. Mani.Kuchibhatla, S. Koteswari, R V S Lakshmi Kumari, Yallapragada Ravi Raju

***Abstract*— The Internet of Things (IoT) facilitates the delivery of intelligent services by sensing, gathering, processing, and exchanging data from millions of linked smart devices. The Internet of Things (IoT), which is based on communication infrastructure, provides real-time cyber-physical device monitoring, control, and sensing, such as electric autos. Traditional communication infrastructure's vulnerability to cyberattacks hampered IoT's capacity to investigate these potential applications. This study proposes an algorithm for monitoring and controlling electric vehicles through the Internet of Things communication network to prevent fake data injection attacks. A state-space model depicts a fully autonomous electric car equipped with a vision system. Intelligent sensors and actuators from the Internet of Things are utilized to monitor and change system conditions, compensating for the large distance between the electric car and the control center. Sensing data is delivered from the vehicle to the central command center via an insecure, attack-prone communication path. The mean square error approach is used to derive states in the most effective state estimation system for comprehending and showing autos. A semi-definite programming approach is used to create an optimal control algorithm to manage the vehicle states. The simulation results show how precisely and successfully the proposed algorithms can foresee and regulate a vehicle's state.**

***Index Terms*—Internet of Things (IoT), cyber-attacks, electric vehicles, communication network, and control center.**

Manuscript Received January 03, 2023; Revised October 25, 2023.

B. Baddu Naik is Assistant Professor in the Department of Electrical and Electronics Engineering, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India.
(E-mail: baddunaik@gmail.com).

V. Venkataiah is Associate Professor in the Department of Computer Science Engineering, CMR College of Engineering & Technology, Hyderabad, Telangana, India.
(E-mail: venkat.vaadaala@gmail.com).

S. Mani.Kuchibhatla is Associate Professor & HOD in the Department of Electrical and Electronics Engineering, ACE Engineering College, Hyderabad, Telangana, India.
(E-mail: drsmanik21@gmail.com)

S. Koteswari is Professor in the Department of Electronics and Communication Engineering, Pragati Engineering College, Surampalem, Kakinada, India, Andhra Pradesh, India.
(E-mail: eshwari.ngr@gmail.com)

R V S Lakshmi Kumari is Associate Professor & HoD in the Department of Electrical and Electronics Engineering, Gayatri Vidya Parishad College of Engineering for Women, Visakhapatnam, Andhra Pradesh, India.
(E-mail: sharmalsk@gmail.com)

Yallapragada Ravi Raju is Assistant professor in the Department of Computer Science and Technology, Madanapalle Institute of Technology and Science, Andhra Pradesh, India.
(E-mail: ravirajuy@mits.ac.in)

I. INTRODUCTION

RESEARCHERS from both academia and industry have found the intelligent transportation system to be an exciting new frontier. Increasing the safety of autonomous vehicles on the road is the main goal of this endeavour. [1]– [2]. It is quite difficult to keep such a system secure and private [3]. Sense, network, and communication technologies are critical to the development of autonomous automated systems. This is due to the fact that the command and control centre and the battery-powered cars are usually situated at significant distances from one another, as seen in Figure 1 [4]. Sensors connected to the Internet of Things (IoT) gather information from moving cars and send it to a command centre using a variety of communication networks [5]–[6].

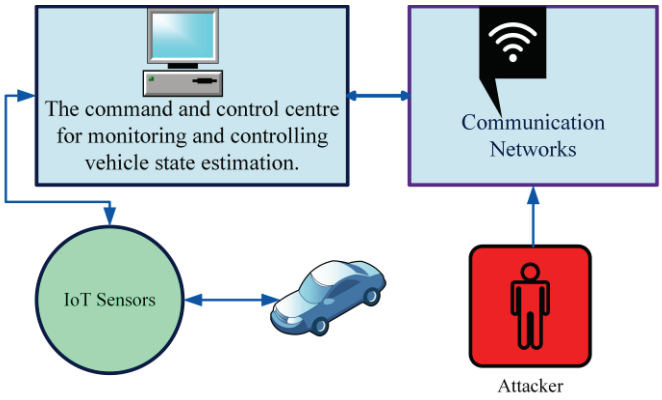

Fig. 1. Designing an electric vehicle based on IoT to protect control centers from cyber attacks

Attacks occur in a communication channel when data is transmitted to a control centre. The attackers inserted bogus data into the connection system in order to track the command and control server. Using the data it has received, the central command estimates the state. In essence, the state estimation technique provides a moment in time for the vehicle's current condition. The state estimate process yields a visual representation of the physical system. In the absence of estimates, the command centre cannot act. Accurate state estimation is necessary for control operations to be effective. This article offers an algorithm for monitoring and controlling electric vehicles online as a solution to this demand.

A. Research Corresponding

Unexpectedly, wearables, automated teller machines, security alarms, garage doors, home appliances, and electric cars are just a few examples of the Internet of Things (IoT) that might be monitored closely by a remote control centre [7]–[9]. All of the electronic gadgets that surround us and enable our daily lives are connected, watched over, and managed by the Internet of Things (IoT) network [4]. In particular, sensors and actuators that are incorporated into physical systems like microgrids and driverless electric cars are part of the Internet of Things [10]. While the actuator precisely regulates the system, the control centre makes use of noisy sensor data to approximate the state of the system [11]. The method of gathering measurement data using installed sensors that are vulnerable to malfunctions and cyberattacks is depicted in Figure 1 [12]. Travel and social disruptions, as well as problems with financial and national security, could result from this [13].

Numerous algorithms are available for tracking and controlling electric cars. The vehicle body slip angle is estimated using the Kalman filter (KF) technique, and the system's states are regulated using a linear quadratic regulator. The idea is further developed in [14]. In this study, we create an H observer for electric vehicles that makes steering and direction corrections based on yaw rate and lateral dynamics data. Furthermore, an extended and unscented KF for EV monitoring is described by the methods in [15]. Luenberger observers for determining vehicle position and shaft torque have been created and validated [16]. The algorithm for evaluating the status of the cyber-physical system is built by [17], considering the possibility of a cyberattack, but no strategy for optimal control is devised.

For use in autonomous vehicle systems, trusted algorithms based on KF and Chi-squared detectors are created [18]. Furthermore, the KF is used in conjunction with watermarking in [19] to identify cyberattacks. In a similar vein, [20] develops decision tree- and neural network-based cyberattack defence strategies for low-resource car systems. To further reduce potential risks to the safety of motor vehicles, an optimisation technique based on mixed-integer linear programming has been devised [21]. Transport layer security and effective handshaking algorithms can currently be used to defend wireless networks, mobile devices, and Internet of Things infrastructures [22]. In order to guard against cyberattacks, the authors of [23] provide a trial-and-error method based on the data collection time and historical LEGO data. We are now in the early stages of developing an efficient algorithm that can both prevent cyberattacks and estimate a vehicle's state via the Internet of Things. For instance, in the context of Internet of Things-based electric vehicles, there are no closed-form formulas for optimal gain and error covariance that account for cyberattacks.

Furthermore, [24] describes how to diagnose a malfunctioning electric vehicle steering actuator. By combining the Takagi-Sugeno control method with the Lyapunov stability approach, [25] controls the vehicle's speed. Furthermore, the Takagi-Sugeno observer was created to simultaneously assess the vehicle's steering and sideslip angles [26]. For lane holding in vision-based autonomous vehicles, a nested proportional-integral-derivative (PID) steering control has been developed [27]. The development of an effective gain-programmed H controller for EV lateral stability followed [28]. In conclusion, [29] suggests an electric vehicle dual-degree-of-freedom control method that combines driver steering and automated lane-keeping. To the best of our knowledge, there is not enough research done on semi-definite programming-based optimum control algorithms for electric vehicle systems.

B. Significant Operations

Taking into consideration cyber-attacks on communication channels, algorithms for state estimation and control are proposed for self-driving electric automobiles in this article. This article's major contributions are summed up as follows:

1) A state-space framework is used to characterise the interplay between the vehicle dynamics and the vision system, and Internet of Things-enabled smart sensors are deployed to collect state information. Sensing data is supplied to the control center via an open communication network.

2) To know and show vehicle states from received signals, an optimal estimation approach is provided, with the mean square error between the real and estimated system states as the chosen metric.

3) Using semi-definite programming, an optimal feedback control system is designed to maintain the vehicle's steady states. The required system states are preserved by employing the planned gain, which is derived via a convex optimization technique, as the feedback gain.

4) The proposed algorithm significantly outperforms the conventional approach in numerical simulations.

II. DESCRIPTION OF THE PROBLEM

It's crucial to keep in mind that the precision and accuracy of the measurements and sensors have a significant impact on the process of estimating the vehicle's state. Installed sensors gather data, but they are vulnerable to cyberattacks and malfunctions [12]. There are safety and national security issues because of the possibility of monetary losses, travel disruptions, and societal upheaval [13]. The identification and mitigation of assaults is one of the biggest challenges in guaranteeing the resilient operation of an Internet of Things (IoT)-based electric vehicle once the necessary precautions have been taken. This essay focuses on the subject of what kind of vehicle state estimate method is resistant to network intrusion, keeping these challenges in mind. How can the state of the system be optimally regulated in the event that an attack targets the IoT's sensing data? In order to address these concerns, this article develops and applies the best algorithms for the state estimation and feedback control systems of autonomous electric vehicles via an Internet of Things communication network, always keeping in mind the potential for malicious data injection assaults. These malicious data are injected into the system by the attackers in an attempt to deceive the network's control centre. We

will discuss a state-space framework in the following part, which will be used to describe a vehicle equipped with an on-board vision system. A later stage of the algorithm development process will make use of this framework.

A. *Space-Based and IoT-Based Systematic Methods of Sensing For Vehicles*

Due to the increased requirement for mobility, there is a rise in both traffic congestion and road hazards, which can aggravate and make drivers nervous. It's possible for cars to become so automated that the driver won't have to perform any tasks at all. Most contemporary cars are equipped with a smart driving aid that can assist in a number of driving situations. It has been demonstrated that these technologies reduce driving stress and reduce the number of traffic accidents [14], [17], and [25]. As a result, a great deal of effort has gone into figuring out how to create control algorithms for intelligent car systems. Finding out how the system is performing at the moment is the first step.

The electric self-driving car of today is outfitted with an advanced array of sensors and actuators. To make things simple, this post starts with a car model that has an integrated visual system. Thanks to its four main state variables, the model can precisely describe the car's motion characteristics. A key component of the dynamic model for vehicle control is the slip angle, or the angle of a wheel with regard to the direction in which it is really travelling [30]. To ascertain the location and shape of the lines, a camera is mounted in the dashboard, directly in front of the driver's side mirror. The leading wheels' angle and yaw moment are used to control the system. In the automated driving mode, the steering angle is maintained at its current value by means of motor torque. The control algorithm cannot be built unless the interaction between the vehicle dynamics and the vision system is modelled using the state-space framework. To do this, the differential equations for the vehicle are described as follows [14]:

$$\beta = 2\frac{C_f}{mV_x}\left(\delta_f - \gamma\frac{l_f}{V_x} - \beta\right) - \frac{\gamma}{mV_x} + \frac{2C_r}{mV_x}\left(\gamma\frac{l_r}{V_x} - \beta\right) \quad (1)$$

$$\gamma = 2\frac{l_f C_f}{I}\left(\delta_f - \gamma\frac{l_f}{V_x} - \beta\right) - \frac{N_z}{I} + \frac{2l_r C_r}{I}\left(\gamma\frac{l_r}{V_x} - \beta\right) \quad (2)$$

Here, C_f /C_r is the front/rear tire cornering stiffness, β is the body slip angle, V_x is the vehicle longitudinal velocity around the center of gravity, *m* is the vehicle mass, δ_f is the front-wheel angle, γ is the vehicle yaw rate, l_r/l_f is the distance between the center of gravity and the rear/front axle, I is the inertia vehicle moment, and N_z is the yaw moment. In-wheel motor (IWM) can generate torque as follows:

$$T_l = F_{rl}r = \frac{mra_x}{2} + \frac{rN_z}{d_r}, T_r = F_{rr}r = \frac{mra_x}{2} - \frac{rN_z}{d_r} \quad (3)$$

Here, T_l/T_r is the rear left/right IWM torque, F_{rl}/F_{rr} is the longitudinal force acting on the rear left/right tire, r is the wheel radius, and d_r is the track width.

The vehicle moves along the road while the on board vision system detects the lane and provides positional data [14]. The heading angle ψ can be described as follows:

$$\varphi = \gamma \quad (4)$$

The lateral offset at the preview point y_l is given by

$$y_l = y_{cg} + sin\varphi l_{pev} \quad (5)$$

Here, y_{cg} is the lateral offset around the center of gravity, l_{pev} is the preview distance, and the approximation is due to the fact that ψ and β are generally very small [14]. The lateral offset around the center of gravity is given by

$$y_{cg} = V_{cg} + sin(\beta + \varphi) \quad (6)$$

Using (4) and (5), and taking the partial derivative of (5) yields

$$y_l = y_{cg} + \varphi l_{pev} \quad (7)$$

Combining (1), (2), (4), and (7), the following discrete-time state-space framework is obtained:

$$X_{k+1} = A_d X_k + B_d u_k + n_k \quad (8)$$

Where x = [β γ ψ y_l] is the system state vector, k is the time step, $A_d = e^{AcT}, B_d = \int_0^T e^{Ac\tau} B_c d\tau$, T is the discretizing sampling time, u = [δ_f N_z] is the system input, and n is the process noise whose covariance matrix is Q. The continuous time state matrix A_c and the input matrix B_c are given by

$$A_c = \begin{bmatrix} -2\frac{C_r+C_f}{mV_x} & 2\frac{C_r l_r - C_f l_f}{mV_x^2} & 0 & 0 \\ -2\frac{C_r l_r + C_f l_f}{I} & 2\frac{-C_r l_r^2 + C_f l_f^2}{IV_x} & 0 & 0 \\ 0 & 1 & 0 & 0 \\ V_x & l_{pre} & V_x & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 2\frac{C_f}{mV_x} & 2\frac{C_f l_f}{I} & 0 & 0 \\ 0 & \frac{1}{I} & 0 & 0 \end{bmatrix}$$

Smart electric vehicles have been identified as a potential option for reducing pollution and carbon dioxide emissions by the transportation sector, the academic community, and environmental activists [1]. Because people are becoming more mindful of the environment and want to limit global warming to a manageable level, there is a growing market for electric vehicles that plug in or run on batteries. IoT-based electric vehicles are something that many believe will be a part of a green, clean, and sustainable smart city. Fundamentally, the intelligent transportation system enhances completely autonomous vehicle security. It offers practical features including intelligent parking and transit, automated car tracking, and real-time traffic information [1, 2, and 31]. Different delivery mechanisms for these services could be implemented using network infrastructure and Internet of Things sensors. The system administrators utilise a suite of Internet-connected smart sensors to monitor and detect the electric vehicle.

$$y_k = C_{xk} + v_k \quad (9)$$

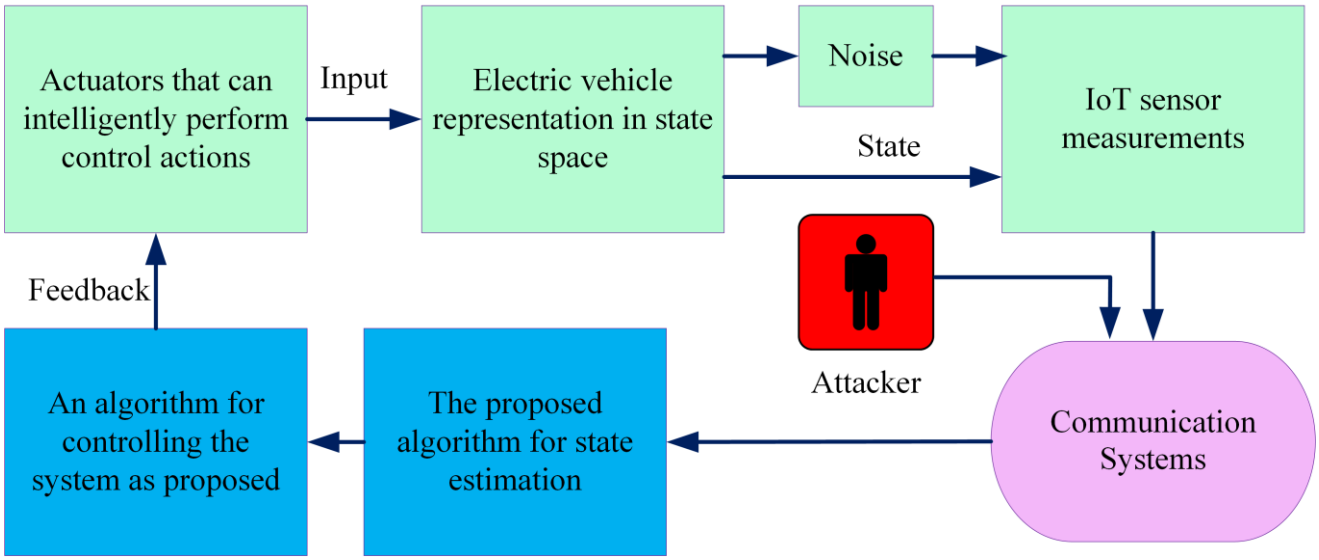

Fig. 2. New methods of communication and algorithms for the Internet of Things

When v is the measurement noise with covariance matrix R, y is the observational data, and C is the sensing matrix, As seen in Figure 2, the sensor processes the raw measurements locally and transmits the measurement innovation through the channel where attacks take place. In an attempt to fool the command and control server, attackers insert malicious data into the network they have targeted. Two algorithms are utilised: control is intended to keep the system in a stable state, and state estimate is designed to give a visual depiction of the vehicle's condition based on the data obtained. The technical aspects of the control action of the smart actuator are described in detail in Figure 2 and the state-space model.

III. STATE ESTIMATION TECHNIQUE UNDER DEVELOPMENT

The optimal state estimation algorithm for knowing and visualizing vehicle states is derived applying the rule of thumb of minimizing the square of the mistake. The following theorem can be used to determine the state of the system, given a state-space framework in (9) and a measurement in (8).

Theorem: Both the a posteriori estimate and the prediction of the state are provided by

$$X_k^- = A_d X_{k-1}, \quad X_k = X_k^- + K z_k \tag{10}$$

Here, x_{k-1} and x_k are the a priori and a posteriori estimated states. The predicted and updated error covariance is given by [31].

$$P_k = A_d P_{k-1} A_d' + Q \tag{11}$$

The gain K minimizes the error dynamic z, leading to an accurate estimated vehicle state over time. The aforementioned state estimation process is described in Figure-2. The proposed control algorithm is designed to regulate the system states after visualizing the vehicle states by an estimation approach. By reducing the error dynamic z, the gain K helps produces reliable estimates of the vehicle's state over time. It is shown in Figure-2 how the aforementioned state estimation procedure works. The proposed control algorithm is meant to regulate the system states after an estimation method is used to visualize the vehicle's current state.

A. Proposed Control Technique

Semi-definite programming is used to design an optimal control algorithm for the vehicle states. The feedback control law is specified in accordance with the separation principle.

$$u_k = G_{xk} \tag{12}$$

According to Figure-2, G represents the feedback gain that must be created. The controlled action is implemented by the actuator. What follows is a description of the closed-loop system:

$$X_{k+1} = (A_d + B_d G) X_k + n_k \tag{13}$$

Consider the following search optimization problem best gain G based on the bounded real lemma in the absence of noise:

$$A_{cl}' P A_{cl} - P + \epsilon < 0, P > 0 \tag{14}$$

$$(A_d + B_d G)' X^{-1} (A_d + B_d G) - X^{-1} + \epsilon < 0 \tag{15}$$

Applying Schur's complement to (15) yields

$$\begin{bmatrix} -X & X(A_d' + B_d' G') & X \\ X(A_d' + B_d' G')' & -X & 0 \\ X & 0 & \in I \end{bmatrix} < 0 \tag{16}$$

Using the method of linear matrix inequalities (LMI), we can solve the aforementioned inequality if we define S = GX. Thus, the aforementioned inequality can be expressed as:

$$\begin{bmatrix} -X & XA_d' + S'B_d^1 & X \\ (XA_d' + S'B_d^1)' & -X & 0 \\ X & 0 & -\in I \end{bmatrix} < 0 \quad (17)$$

In terms of X and S, we have here a case of LMI. It is possible to obtain X and S by solving (17). To conclude, the ideal gain is established by

$$G = X^{-1}S \quad (18)$$

The YALMIP programme can solve this problem quickly and accurately. In the following section, we examine the efficacy of the proposed approach.

IV. AN ASSESSMENT OF THE RESULTS AND DISCUSSIONS GLEANED FROM THE SIMULATIONS

The complete simulation can be seen illustrated by the method indicated in Figure 2. When the automobile and IoT sensing models are adequately specified, it will be simple to derive the estimation and control methods that are presented from the data that was received. Every cycle (11) includes revisions to (10), which are used for performing an evaluation of the current state, and (11), which are intended for the error covariance process. After working through (17), you will arrive at (18), which is the optimal feedback gain. The predicted gain exerts a precise amount of control over the current state of the system. In order to account for the possibility of an attack including the injection of fake data, the simulation models both the typical operation of the sensor as well as its failure.

The communication network is the principal target of attacks between time steps 10 and 20, and sensor failures are not taken into consideration during this time period. The results of the simulations presented in Figure 3 demonstrate that the methodology that was suggested achieves higher levels of performance than the one that is currently considered to be state-of-the-art. In contrast to the current method, the strategy that has been developed is capable of quickly locating the best answer while simultaneously reducing the number of estimating errors. There will be convergence between the estimated and true states after the dynamics of the estimating error have reached a stable state. Graphic representations of the vehicle's dynamic state reactions are shown in Figures 4–6. As can be seen in this illustration, the proposed algorithm is capable of making an accurate prediction of the state of the system. Figure 5 depicts the estimated value of the vehicle slip angle at its current speed. In comparison, the proposed method only requires approximately 22 iterations to track the system state (time step k sampling time T = 0.022 s), whereas the existing method requires approximately 150 iterations (kT = 0.15 s) to do the same thing. All of the other states of the vehicle are also subject to the same level of estimation precision.

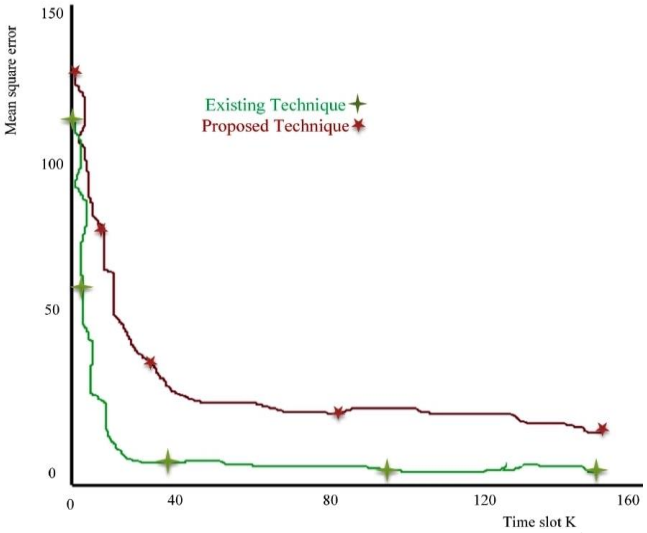

Fig. 3. Results are compared to mean square error in the absence of sensor faults

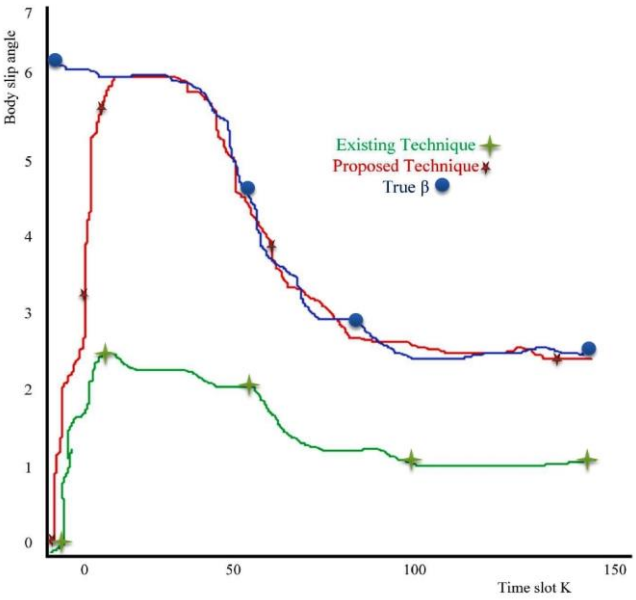

Fig. 4. Body slips angle β assessment in the absence of sensor faults

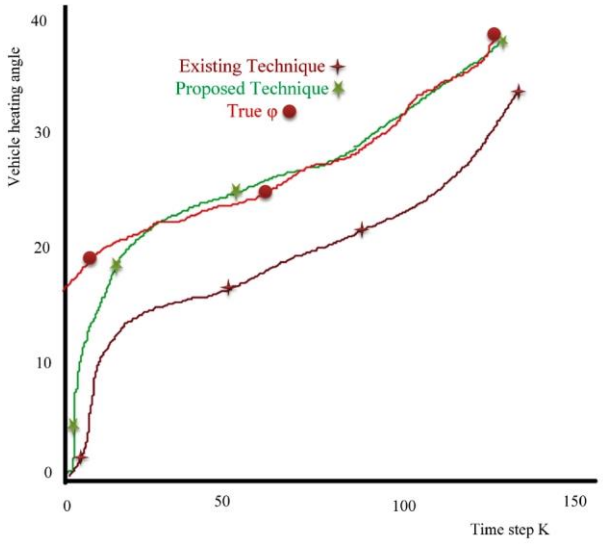

Fig. 5. Vehicle heading angle ψ assessment in the absence of sensor faults

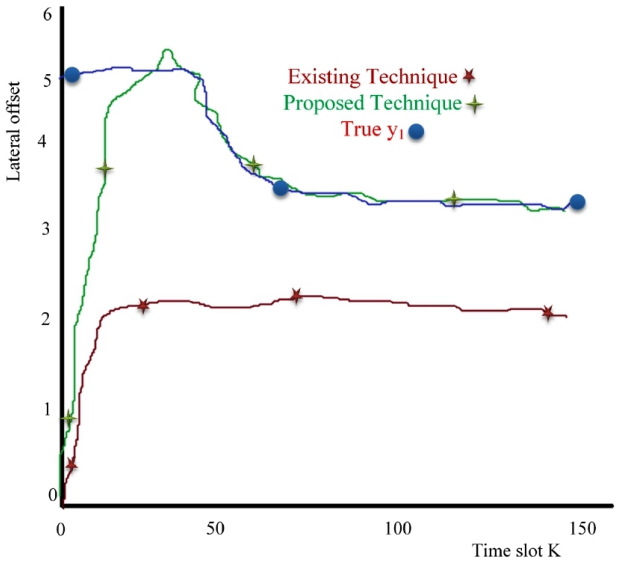

Fig.6. Without sensor faults, lateral offset yl and its estimation

Sometimes the sensing components of the system are unable to get an accurate readout of the state of the system because of external impacts or sensor faults. In Figure 7, we see an illustration of the mean square error that occurs between the estimated and actual states of the system when sensors fail or when there are cyberattacks. Figures 8–10 also show the reactions of the system states to the time steps that have been taken in the experiment. The way that was proposed performs noticeably better than the regular method that was described earlier. In addition, it is obvious that the strategy that was presented needs more time in the event that there is no problem, in comparison to the amount of time it needs in the event that there is a cyberattack or a sensor malfunction.

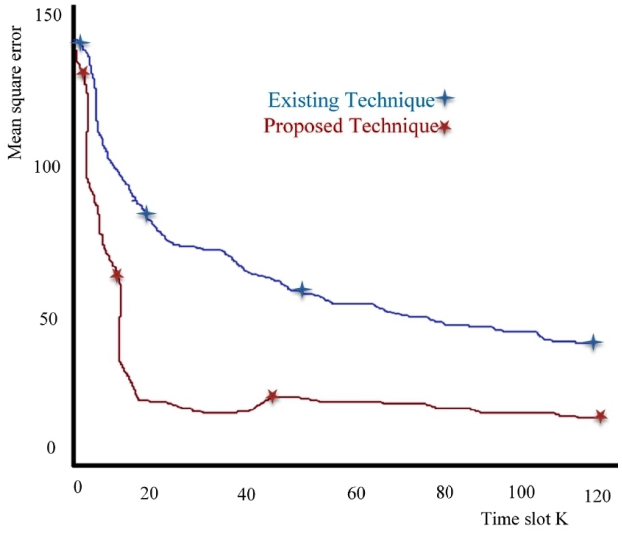

Fig. 7. Mean square error is compared to sensor fault conditions

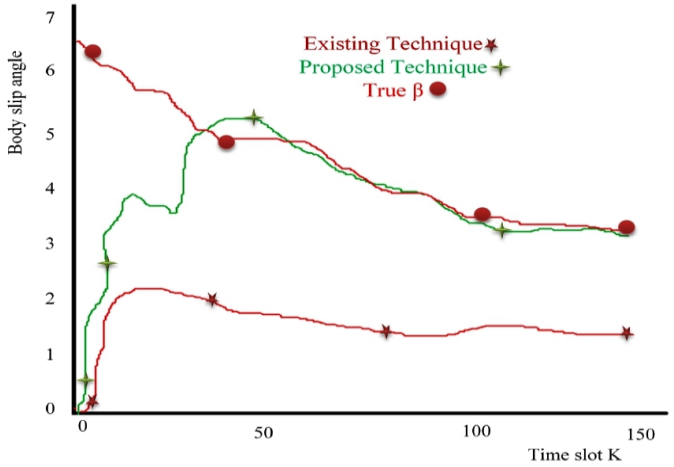

Fig. 8. Angle of body slip β and its estimation under sensor fault conditions

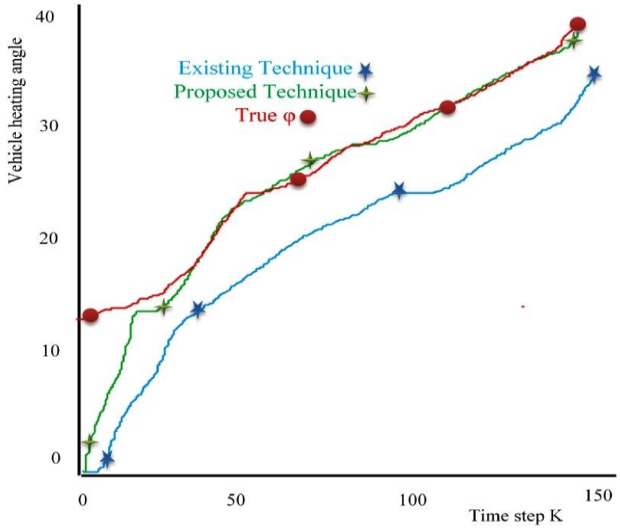

Fig. 9. The estimation of the vehicle's heading angle ψ under imperfect sensor conditions

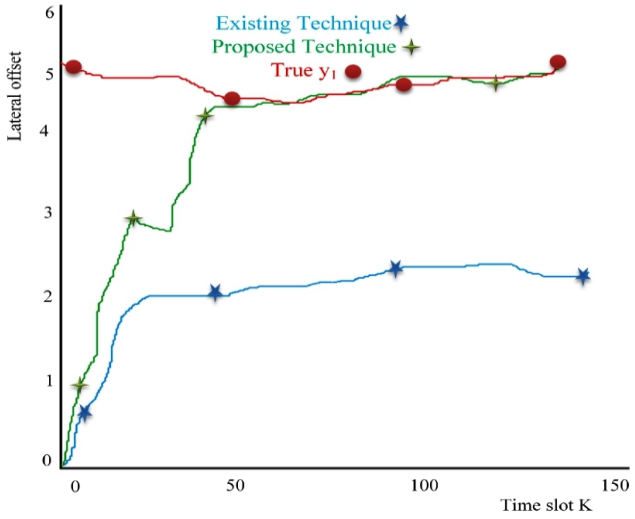

Figure-10: Lateral offset yl and its estimation in the presence of sensor fault conditions

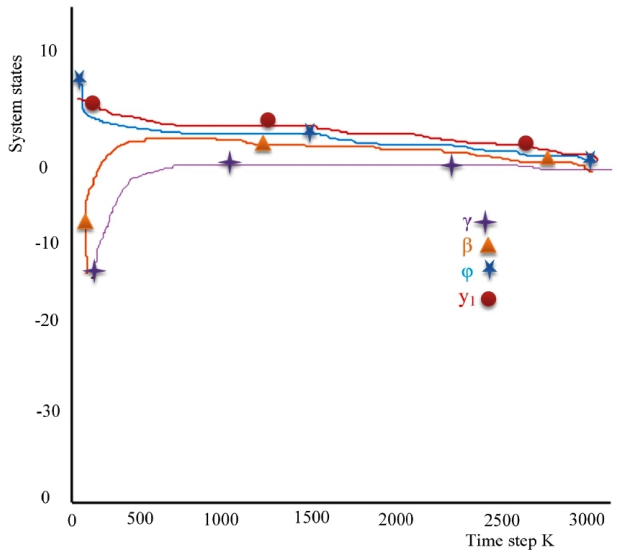

Fig. 11. Maintaining the trajectories of the vehicle's states

The goal of a control algorithm is typically to reduce as much as possible the amount of time required for the states of the system to converge on a stable average. The results that were produced by making use of the suggested control strategy are presented here in Figure 11. When employing the provided method, it is clear that the proposed strategy may effectively control the states of the system in a time period that is shorter than 1600 iterations (kT = 1.6 seconds). It is essential to keep in mind that this period of stabilisation lasts for a shorter amount of time than the customary three seconds [25]. This is as a result of the fact that the recommended controller possesses the intelligence to figure out what the ideal feedback gain should be in order to maintain the system's stability.

V. CONCLUSION

Algorithms for state estimation and control optimisation were developed with the intention of facilitating the monitoring and management of a cyberattack that was launched against an electric vehicle that was powered by the Internet of Things (IoT). The dynamics of the vehicle were defined within a state-space framework with the help of the onboard vision system, and then the Internet of Things' smart sensors were utilised to sense the system's states. A breach occurred in a channel that was being utilised to send information. During the process of developing the suggested algorithms, the notion of mean square error as well as semi-definite programming were utilised. The results of the simulation show how quickly and accurately the state of the system can be estimated and stabilised by utilising the suggested estimation and control techniques. This information will be helpful to the engineers who create the systems for driverless vehicles. In the not too distant future, the suggested methods will be put through experimental testing to validate whether or not they are effective.

REFERENCES

[1] H. Zhang, G. Zhang and J. Wang, "Sideslip Angle Estimation of an Electric Ground Vehicle via Finite-Frequency H∞ Approach," in IEEE Transactions on Transportation Electrification, vol. 2, no. 2, pp. 200-209, June 2016.

[2] C. Chen, L. Liu, T. Qiu, Z. Ren, J. Hu and F. Ti, "Driver's Intention Identification and Risk Evaluation at Intersections in the Internet of Vehicles," in IEEE Internet of Things Journal, vol. 5, no. 3, pp. 1575-1587, June 2018.

[3] A. Nourian and S. Madnick, "A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 2-13, 1 Jan.-Feb. 2018.

[4] M. T. Khan, D. Serpanos and H. Shrobe, "ARMET: Behavior-Based Secure and Resilient Industrial Control Systems," in Proceedings of the IEEE, vol. 106, no. 1, pp. 129-143, Jan. 2018.

[5] J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 439-449, Feb. 2018.

[6] C. Arcadius Tokognon, B. Gao, G. Y. Tian and Y. Yan, "Structural Health Monitoring Framework Based on Internet of Things: A Survey," in IEEE Internet of Things Journal, vol. 4, no. 3, pp. 619-635, June 2017.

[7] A. Singh and M. Singh, "An empirical study on automotive cyber attacks," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), 2018, pp. 47-50.

[8] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, and W. Zhao, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet Things J., vol. 4, no. 5, pp. 1125–1142, Oct. 2017.

[9] W. Shi, J. Cao, Q. Zhang, Y. Li and L. Xu, "Edge Computing: Vision and Challenges," in IEEE Internet of Things Journal, vol. 3, no. 5, pp. 637-646, Oct. 2016.

[10] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A survey," IEEE Internet Things J., vol. 3, no. 1, pp. 70–95, Feb. 2016.

[11] L. Yu, D. Xie, T. Jiang, Y. Zou, and K. Wang, "Distributed real-time HVAC control for cost-efficient commercial buildings under smart grid environment," IEEE Internet Things J., vol. 5, no. 1, pp. 44–55, Feb. 2018.

[12] A. S. Musleh, H. M. Khalid, S. M. Muyeen and A. Al-Durra, "A Prediction Algorithm to Enhance Grid Resilience Toward Cyber Attacks in WAMCS Applications," in IEEE Systems Journal, vol. 13, no. 1, pp. 710-719, March 2019.

[13] Y. Wang, B. M. Nguyen, H. Fujimoto, and Y. Hori, "Multirate estimation and control of body slip angle for electric vehicles based on onboard vision system," IEEE Trans. Ind. Electron., vol. 61, no. 2, pp. 1133–1143, Feb. 2014.

[14] M. N. Kurt, Y. Yılmaz and X. Wang, "Distributed Quickest Detection of Cyber-Attacks in Smart Grid," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 8, pp. 2015-2030, Aug. 2018.

[15] L. Wang, L. Wang, C. Liao, and W. Zhang, "Research on multiple states joint estimation algorithm for electric vehicles under charge mode," IEEE Access, vol. 6, pp. 40143–40152, 2018.

[16] C. Lv, Y. Liu, X. Hu, H. Guo, D. Cao, and F.-Y. Wang, "Simultaneous observation of hybrid states for cyber-physical systems: A case study of electric vehicle powertrain," IEEE Trans. Cybern., vol. 48, no. 8, pp. 2357–2367, Aug. 2018.

[17] M. M. Rana, "Attack Resilient Wireless Sensor Networks for Smart Electric Vehicles," in IEEE Sensors Letters, vol. 1, no. 2, pp. 1-4, April 2017.

[18] R. G. Dutta, F. Yu, T. Zhang, Y. Hu, and Y. Jin, "Security for safety: A path toward building trusted autonomous vehicles," in Proc. Int. Conf. Comput.-Aided Design, 2018, pp. 92–97.

[19] V. Marquis et al., "Toward attack-resilient state estimation and control of autonomous cyber-physical systems," in Proc. Syst. Inf. Eng. Design Symp., 2018, pp. 70–75.

[20] A. Sargolzaei, C. D. Crane, A. Abbaspour and S. Noei, "A Machine Learning Approach for Fault Detection in Vehicular Cyber-Physical Systems," 2016 15th IEEE International Conference on Machine Learning and Applications (ICMLA), pp. 636-640, 2016,

[21] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A riskbased optimization model for electric vehicle infrastructure response to cyber-attacks," IEEE Trans. Smart Grid, vol. 9, no. 6, pp. 6160–6169, Nov. 2018.

[22] J. Cai et al., "A handshake protocol with unbalanced cost for wireless updating," IEEE Access, vol. 6, pp. 18570–18581, 2018.

[23] K. Yang et al., "Enhanced resilient sensor attack detection using fusion interval and measurement history," in Proc. Int. Conf. Hardw. Softw. Codesign Syst. Synth., 2018, pp. 1-3.

[24] H. Zhang and J. Wang, “Active steering actuator fault detection for an automatically-steered electric ground vehicle,” IEEE Trans. Veh. Technol., vol. 66, no. 5, pp. 3685–3702, May 2017.
[25] A. T. Nguyen, C. Sentouh, J.-C. Popieul, and B. Soualmi, “Shared lateral control with on-line adaptation of the automation degree for driver steering assist system: A weighting design approach,” in Proc. Int. Conf. Decis. Control, 2015, pp. 857–862.
[26] Pengwei Wang, Tianqi Gu, Binbin Sun, Rui Dang, Zhenwei Wang, and Weichong Li, "Energy Management of Electromechanical Flywheel Hybrid Electric Vehicle Based on Condition Prediction," Engineering Letters, vol. 30, no.4, pp1269-1277, 2022.
[27] R. Marino, S. Scalzi, G. Orlando, and M. Netto, “A nested PID steering control for lane keeping in vision based autonomous vehicles,” in Proc. Int. Conf. Amer. Control Conf., 2009, pp. 2885–2890.
[28] Pengwei Wang, Tianqi Gu, Binbin Sun, Rui Dang, Zhenwei Wang, and Weichong Li, "Performance Analysis of Electromechanical Flywheel for Electric Vehicles Based on Planetary Gear Mechanism," Engineering Letters, vol. 30, no.4, pp1521-1530, 2022.
[29] V. Cerone, M. Milanese, and D. Regruto, “Combined automatic lanekeeping and driver’s steering through a 2-DOF control strategy,” IEEE Trans. Control Syst. Technol., vol. 17, no. 1, pp. 135–142, Jan. 2009.
[30] M. M. Rana and R. Bo, “IoT-based improved human motion estimations method under cyber attacks,” IEEE Internet Things, to be published.
[31] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, “Optimal linear cyberattack on remote state estimation,” IEEE Trans. Control Netw. Syst., vol. 4, no. 1, pp. 4–13, Mar. 2017.