Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTERNET OF THINGS FOR EFFORT ESTIMATION AND CONTROLLING THE STATE OF AN ELECTRIC VEHICLE IN A CYBER ATTACK ENVIRONMENT

BADDU NAIK BHUKYA[1], VUTUKURI SARVANI DUTI REKHA[2], VENKATA KRISHNAKANTH PARUCHURI[3], ASHOK KUMAR KAVURU[3] and KADIYALA SUDHAKAR[3]

[1]Assistant Professor, Department of Electrical and Electronics Engineering,

Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India.

[2]Assistant Professor, Department of Electronics and Communication Engineering,

Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India.

[3]Assistant Professor, Department of Electronics and Communication Engineering,

R. V. R. & J. C. College of Engineering, Guntur, Andhra Pradesh, India.

E-mail: [1]baddunaik@gmail.com, [2]vsdrekha@gmail.com, [3]pvkrishnakanth@rvrjc.ac.in
[3]kashokkumar@rvrjc.ac.in, and [3]kadiyalasudhakar@rvrjc.ac.in

ABSTRACT

The Internet of Things (IoT) lets millions of smart devices sense, gather, process, and exchange data to provide intelligent services. IoT-based communication infrastructure allows cyber-physical devices like electric cars to sense, monitor, and be controlled remotely. IoT cannot explore these uses due to cyberattacks on traditional communication infrastructure. This paper suggests an algorithm for monitoring and managing electric vehicles via the Internet of Things while preventing false data-injection attacks. First, a vision-equipped fully autonomous electric vehicle state-space model is described. Smart sensors and actuators in the Internet of Things infrastructure watch and adjust system states to compensate for the long distance between the electric vehicle and the control centre. Vehicle sensing data is sent to a central command centre via a vulnerable communication route. The mean square error principle yields the best state estimation method for visualising vehicle states. An optimal control algorithm manages car states using semi-definite programming. Simulations demonstrate how well the proposed algorithms can foresee and control vehicle states.

Keywords: *Internet Of Things (Iot), Cyber-Attacks, Electric Vehicles, Communication Network, Control Center.*

1. INTRODUCTION

The intelligent transportation system excites academic and business researchers. This research improves autonomous car road safety [1]–[2]. Maintaining system secrecy and safety is difficult [3]. Autonomous automated systems require sensing, networking, and communication tools. Figure-1 [4] shows that the electric car and monitoring control centre are usually far apart. Vehicle IoT devices send data to the command centre via various communication networks [5]–[6].

Communication channels are attacked when data is sent to control centres. Attackers place false data on the communication network to fool the command and control server. The control centre estimates mood using data. State estimation provides a car state snapshot. State estimation visualises the real system. The command centre needs figures to act. Control requires exact state estimation. This paper proposes an online algorithm to track and manage electric vehicles.

1.1 The Related works

The Internet of Things (IoT) could help remote control centres oversee smart physical systems like wristwatches, vending machines, emergency alarms, garages, home appliances, and electric vehicles [7]–[9]. The IoT network connects, monitors, and controls all of our daily electronic gadgets [4]. Sensors and actuators in micro grids and autonomous electric cars make up the Internet

Journal of Theoretical and Applied Information Technology
31st May 2023. Vol.101. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of Things [10]. The actuator controls the system precisely, while the control centre estimates system states using noisy sensing input [11]. Figure-1 shows how sensors that can fail and be hacked gather measurement data [12]. This could upset national and financial security, travel, and society [13].

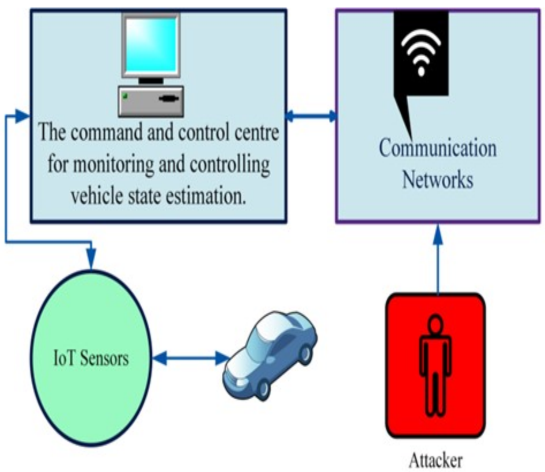

Figure 1: Designing an electric vehicle based on IoT to protect control centers from cyber attacks

Many algorithms watch and control electric vehicles. The linear quadratic regulator controls system states, and the Kalman filter (KF) algorithm estimates car body slip angle. In [14], a lateral dynamic and yaw rate-based electric vehicle H observer is created. [15] also presents extended and unscented KF algorithms for tracking electric cars. The verified Luenberger observer estimates car position and shaft torque [16]. [17]'s method for estimating the cyber-physical system's state accounts for a cyber-attack, but no optimal control algorithm is created.

Autonomous car systems use KF and Chi-squared detector-based algorithms [18]. In [19], the KF and watermarking spot cyberattacks. [20] use neural networks and decision trees to defend low-resource vehicle systems from cyberattacks. An optimization approach using mixed-integer linear programming reduces motor vehicle safety risks [21]. Transport layer security and efficient handshaking methods protect vehicle networks, IoT mobiles, and wireless terminals [22]. Based on LEGO data and information gathering interval, a trial-and-error strategy for resilient cyber-attacks is offered [23]. An algorithm that uses the Internet of Things to estimate vehicle state and defend against cyberattacks is still in development. No closed-form expressions for optimal gain and error covariance in IoT-based electric vehicles allow for cyber-attacks. [24] also identifies faulty electric car steering actuators. [25] regulates car speed with Takagi–Sugeno control and Lyapunov stability. The Takagi–Sugeno observer estimated car steering and sideslip angles simultaneously [26]. Vision-based autonomous cars use nested proportional-integral-derivative (PID) steering controls for lane keeping [27]. Electric car lateral stability control was improved in [28] with a gain scheduled H controller. Finally, [29] suggests a two-degrees-of-freedom electric vehicle control strategy that combines automatic lane-keeping with driver steering. Semi-definite programming-based optimal control algorithms for electric car systems are rarely discussed.

1.2 Important Contributions

In this article, state estimation and control algorithms for autonomous electric automobiles are proposed. These algorithms take into account the possibility of cyberattacks on communication channels. The following is a synopsis of the most important accomplishments made by this article:

A state-space framework is used to model the interaction between the dynamics of the vehicle and the vision system. Internet of Things–enabled smart sensors are distributed to capture state information. When information is gathered from sensors, it is sent to the command centre through a communication network that is open to the possibility of infiltration.

The mean square error between the actual system states and the estimated system states is suggested as the metric of choice to serve as the basis for an optimal estimation algorithm that will be used to determine and display the states of the vehicle based on the received signals.

Through the use of semi-definite programming, an optimal feedback control algorithm is developed in order to stabilise the various conditions of the vehicle. A convex optimization procedure is used to acquire the feedback gain, and the designed gain is then applied in order to keep the desired system states stable.

In the numerical simulations, the proposed algorithm demonstrates substantially better performance than the traditional method.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. COMPLETE SET OF THE CHALLENGING TASK

It is essential to emphasise the fact that the precision and accuracy of the measurements as well as the sensors play a significant part in the process of estimating the state of the vehicle. Installed sensors are responsible for data collection, but it is possible for them to malfunction or come under attack online [12]. Concerns about public safety and national security have been raised as a result of the possibility of monetary losses, travel disruptions, and social unrest [13]. After taking the necessary precautions, one of the most challenging aspects of ensuring the resilient operation of an IoT-based electric vehicle is the detection and mitigation of attacks. This is one of the most significant challenges. In light of these challenges, the focus of this article shifts to the questions of what kind of vehicle state estimation algorithm can withstand cyber-attacks and what kind of control scheme can most effectively regulate the system states when the Internet of Things' sensing information is under attack. This article provides the answers to these questions by designing and implementing the most effective state estimation and feedback control algorithms for autonomous electric vehicles that can be used over an Internet of Things communication network. These algorithms were designed and implemented with the possibility of malicious data injection attacks always in mind. The malicious data is intentionally introduced into the system by the attackers so that they can deceive the control centre of the network. In the following part of this article, we will discuss a state-space framework that will be utilised to represent the model of a vehicle that is equipped with an on-board vision system. In a later stage of the algorithm development process, we will make use of this framework.

2.1 Space-Based and Internet of Things-Based Vehicle Sensing Systems

Traffic congestion and road dangers, caused by increased mobility, can make drivers anxious and irritable. Vehicle technology may make drivers obsolete. Most modern cars have an intelligent driver-assistance device. These devices reduce driver fatigue and traffic accidents [14, 17, 25]. Because of this, intelligent car control algorithm design has been a major focus. Assessing system performance is the first move.

Modern electric self-driving vehicles have advanced sensing and actuators. To simplify, this piece uses the vehicle model with a built-in vision system. The model's four main state variables accurately describe car motion. The dynamic model for car control relies on a wheel's slip angle [30]. The lines are detected by a dashboard camera in front of the driver's side mirror. Leading tyre yaw and angle control the system. Motor power maintains steering angle in automatic driving mode. After modelling the vehicle dynamics-vision system interaction in the state-space framework, the control algorithm can be created. Define the vehicle's differential equations 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 yl is given by

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

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

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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

$$X_{k+1} = A_d X_k + B_d u_k + n_k \tag{8}$$

Where x = [β γ ψ y_l] is the system state vector, k is the time step, $A_d = e^{A_c T}, B_d = \int_0^T e^{A_c \tau} B_c d\tau$, 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 cars may reduce pollution and carbon dioxide emissions, according to academics, environmentalists, and transportation professionals [1]. Due to environmental awareness and the wish to limit global warming, many people now drive battery-powered or plug-in electric cars. Many want IoT-based electric cars in a green, clean, and sustainable smart city. The intelligent transportation system secures fully autonomous cars. It provides automated car tracking, smart fares and parking, and real-time traffic updates [1–31]. These services could be delivered using IoT devices and networks. Smart Internet-connected sensors monitor the electric car for the system's operators.

$$y_k = C_{xk} + v_k \tag{9}$$

The sensing matrix C, sighting information y, and measurement noise v with covariance matrix R are given. Figure-2 shows that the sensor processes raw measurements locally and transmits measurement innovation over the attack channel. Attackers fool the command and control server by injecting harmful data into the targeted network. State prediction uses data to visualise the vehicle's state, while control maintains system stability. Figure-2 and the state-space model explain how the smart actuator controls.

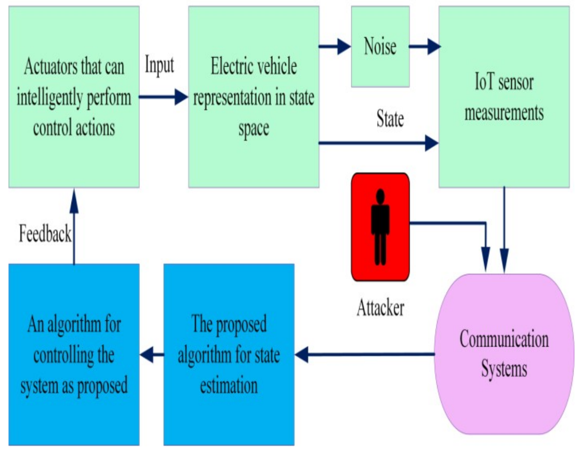

Figure 2: New methods of communication and algorithms for the Internet of Things

3. EMERGING TECHNIQUE FOR ESTIMATING STATES

The mean square error concept guides the optimal state estimation algorithm for vehicle state visualisation. The following theorem can be used to find the system's state given a state-space framework in (9) and a measurement in (8).

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

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].

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

Gain K minimises error dynamic z, resulting in precise vehicle state estimates over time. Figure-2 depicts state prediction. After estimating car states, the proposed control algorithm regulates system states. Gain K improves vehicle state estimates by lowering the error dynamic z. Figure-2 illustrates the state estimation process. After estimating the vehicle's state, the proposed control programme regulates system states.

3.1 Control Method

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.

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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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:

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

Here is an optimization problem to find the best gain G based on the bounded real lemma in the absence of noise:

$$A'_{cl} P A_{cl} - P + \epsilon < 0, P > 0 \quad (14)$$

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

Applying Schur's complement to (15) yields

$$\begin{bmatrix} -X & X(A'_d + B'_d G') & X \\ X(A'_d + B'_d G')' & -X & 0 \\ X & 0 & \in I \end{bmatrix} < 0 \quad (16)$$

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. After solving (17), one can get X and S. Finally, the optimal gain is determined 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.

4. EVALUATING AND DISCUSSING SIMULATION RESULTS

Figure-2 shows the modelling process. After correctly representing the vehicle and IoT sensing models, the proposed estimation and control algorithms use the received information. Each cycle updates state estimation (10) and error covariance method (11). (11). Solving (17) yields the optimal feedback gain (18). The intended gain perfectly controls system state. The simulation is run with and without sensor fault conditions to allow for false data injection [3].

Attackers ignore sensor errors in time steps 10–20. Figure-3 shows simulation data showing the proposed algorithm outperforms the state-of-the-art method. The proposed algorithm minimises estimation errors better than the present method [17]. When estimation error dynamics are tamed, true and predicted states converge. Images 4–6 depict vehicle dynamics. Here, the proposed algorithm correctly predicts system states. Figure 5 estimates the car slip angle. The current method requires over 150 iterations (k×T = 0.15 s) to trace system state, while the proposed algorithm only needs 22 (time step k sampling time T = 0.022 s). Other vehicle states use these prediction precisions.

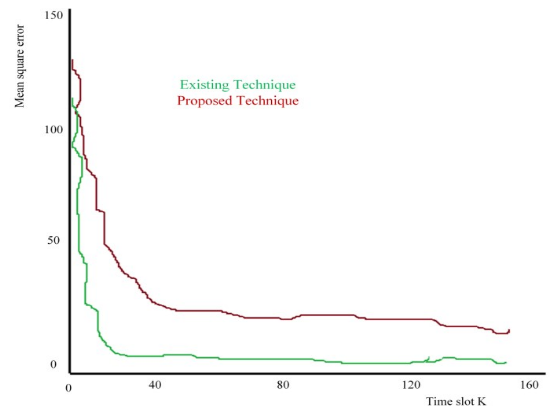

Figure 3: Results are compared to mean square error in the absence of sensor faults.

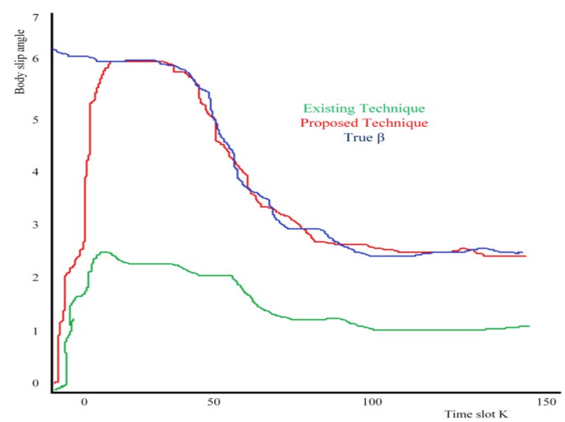

Figure 4: Body slip angle β assessment in the absence of sensor faults.

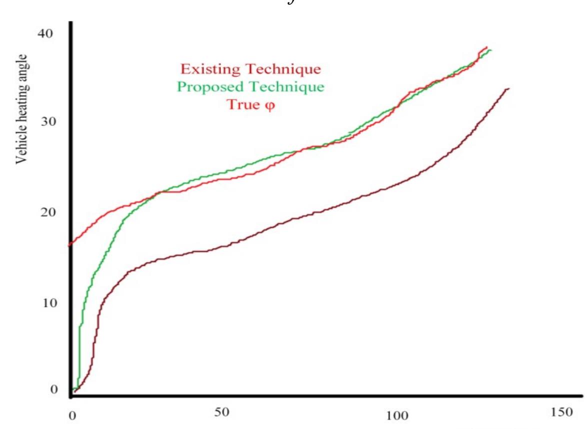

Figure 5: Vehicle heading angle ψ assessment in the absence of sensor faults.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

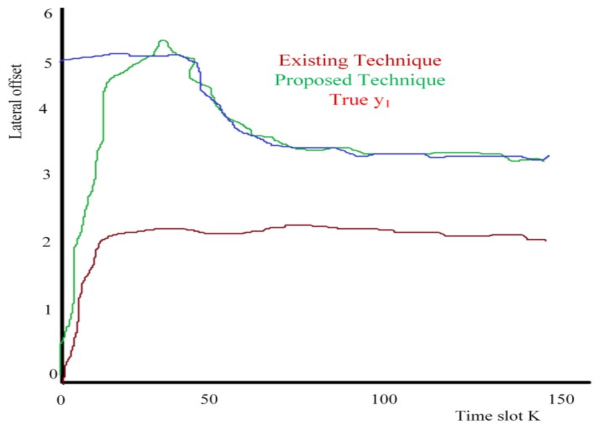

Figure 6: Without sensor faults, lateral offset yl and its estimation

Environmental factors and sensor errors can prevent sensing components from accurately assessing system state. Figure-7 shows the mean square error between real and estimated system states under sensor fault and cyber-attack conditions. Figures 8–10 show system state reactions to time steps. It outperforms the conventional way. The proposed method takes longer when there is no sensor error or cyber-attack than when there is.

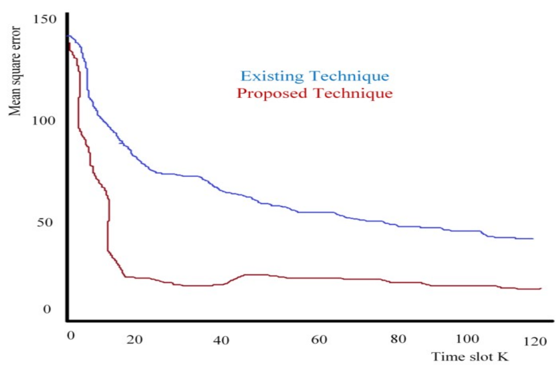

Figure 7: Mean square error is compared to sensor fault conditions.

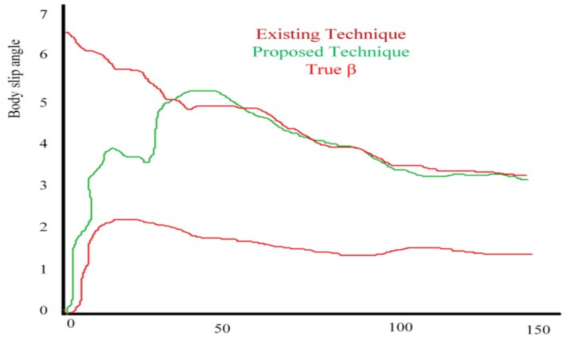

Figure 8: Angle of body slip β and its estimation under sensor fault conditions.

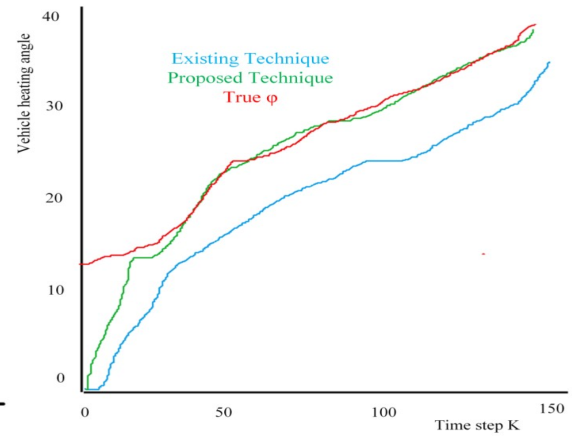

Figure 9: The estimation of the vehicle's heading angle ψ under imperfect sensor conditions

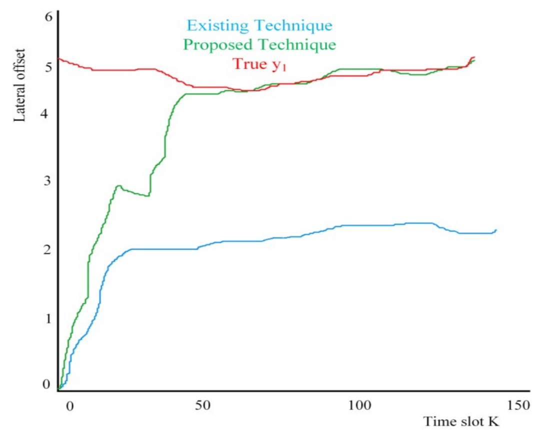

Figure 10: Lateral offset yl and its estimation in the presence of sensor fault conditions

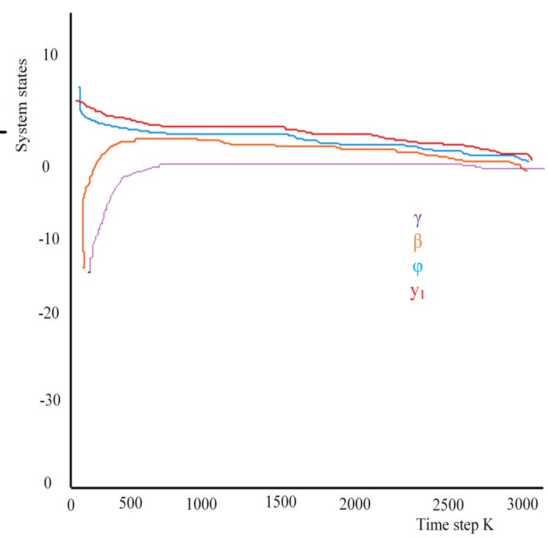

Figure 11: Maintaining the trajectories of the vehicle's states.

Control algorithms usually normalise system states swiftly and efficiently. Figure-11 shows the proposed control method results. The proposed method can control system states in under 1600 iterations (k×T = 1.6 s). It takes less than three seconds to stabilise [25]. The proposed controller intelligently determines the optimum feedback gain for system stability.

5. CONCLUSION

In order to successfully manage a cyberattack on an electric car that was built on the Internet of Things (IoT), optimal state estimation and control algorithms were necessary. After the on-board vision system expressed car dynamics within a state-space framework, the Internet of Things' smart sensors were able to detect the system's current state. assault on the communication highway The techniques were developed through the use of semi-definite programming and the mean square error theory. The suggested estimation and control algorithms have been shown to be able to accurately forecast and stabilise system states through the use of simulations. Designers of systems for autonomous vehicles can benefit from reading this article. Experiments will be done to determine whether or not the suggested procedures 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]. B. Zhang, H. Du, J. Lam, N. Zhang, and W. Li, "A novel observer design for simultaneous estimation of vehicle steering angle and sideslip angle," IEEE Trans. Ind. Electron., vol. 63, no. 7, pp. 4357–4366, Jul. 2016.

[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]. X. J. Jin, G. Yin, and N. Chen, "Gain-scheduled robust control for lateral stability of four-wheel-independent-drive electric vehicles via linear parameter-varying technique," Mechatronics, vol. 30, pp. 286–296, Sep. 2015.

[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.