


# IoT-Based Electric Vehicle State Estimation and Control Algorithms Under Cyber Attacks

Md Masud Rana 

**Abstract**—In order to provide intelligent services, the Internet-of-Things (IoT) facilitates millions of smart devices to be enabled with network connectivity to sense, collect, process, and exchange information. Based on the communication infrastructure, the IoT can allow cyber-physical devices, such as an electric vehicle, to sense, monitor, and control from the remote control center in real time. Unfortunately, the traditional communication infrastructure is vulnerable to cyber attacks, so it is a challenging task for the IoT to explore these applications. In order to overcome the problem, this article proposes an algorithm for monitoring and controlling the electric vehicle using the IoT communication network considering false data-injection attacks. First, the driverless electric vehicle with onboard vision system is represented by a state-space framework. As the electric vehicle and monitoring control center are far away, the IoT-embedded smart sensors and actuators are used to measure and control the system states. The vehicle sensing information is transmitted to the control center over an unreliable communication channel where attacks happen. Based on the mean square error principle, the optimal state estimation algorithm is derived to know and visualize the vehicle states. In order to regulate the vehicle states, the optimal control algorithm is designed based on the semidefinite programming approach. The simulation results show that the proposed algorithms are able to properly estimate and regulate the vehicle states within a short period of time.

**Index Terms**—Control center, cyber attacks, dynamic state estimation, electric vehicle, Internet-of-Things (IoT), linear matrix inequality (LMI), semidefinite programming, vision systems.

## I. INTRODUCTION

THE intelligent transportation system is an attractive area of research both in academic and industrial researchers. The main aim of this effort is enhancing the driving safety for automated vehicles [1]–[3]. Ensuring the security and privacy of such a system is a major challenge [4], [5]. In order to design driverless automated systems, the sensing, networking, and communication technologies play a vital role. This is due to the fact that the electric vehicle and monitoring control center are generally far away as shown in Fig. 1 [6], [7]. It can be seen that the vehicle information is sensed by Internet-of-Things (IoT) sensors and transmitted to the control center through communication networks [8]–[10]. The attacks occur in a communication channel during the transmission of

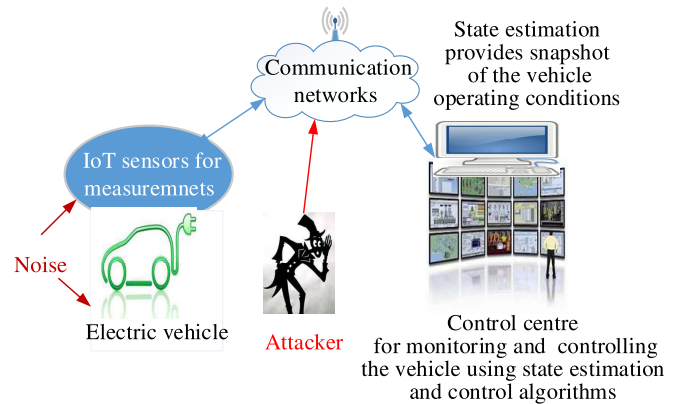


Fig. 1. IoT-based electric vehicle for control center design under cyber attacks.

information to the control center. The attackers inject malicious information into the communication network to mislead the control center. Based on the received information, the state estimation is performed at the control center. Basically, the state estimation algorithm provides a snapshot of the vehicle operating conditions. In other words, visualization of the physical system is obtained by the state estimation process. Without an estimation, the control center cannot take any action. Therefore, the state estimation is of paramount importance to take effective control actions. Driven by this motivation, this article proposes an algorithm for monitoring and controlling the electric vehicle using the IoT technologies under cyber attack conditions.

## A. Related Work

Interestingly, the IoT is the potential technology that will be able to closely monitor the smart physical systems, such as wristwatches, vending machines, emergency alarms, garage, home appliances, and electric vehicles from the remote control center [11]–[14]. It can be observed that all surrounding electronic devices to facilitate our daily life operations are remotely connected, monitored, and controlled to the IoT network [7]. Specifically, the IoT-embedded sensors and actuators are integrated into the physical systems, such as automated electric vehicles and microgrids [15]. The noisy version of the sensing information is used at the control center to estimate the system states while the actuator is used to properly control them [16]. For doing this, the measurement information

Manuscript received June 21, 2019; revised August 2, 2019; accepted September 18, 2019. Date of publication October 8, 2019; date of current version February 11, 2020.

The author is with the Electrical and Computer Engineering, Missouri University of Science and Technology, Rolla, MO 65409 USA (e-mail: mrana928@yahoo.com).

Digital Object Identifier 10.1109/JIOT.2019.2946093

2327-4662 © 2019 IEEE. Personal use is permitted, but republication/redistribution requires IEEE permission.  
See [http://www.ieee.org/publications\\_standards/publications/rights/index.html](http://www.ieee.org/publications_standards/publications/rights/index.html) for more information.

is obtained by installed sensors, which are vulnerable to malfunction and cyber attacks as shown in Fig. 1 [17], [18]. This raises safety and national security concerns which may lead to financial losses, travel, and social problems [19], [20].

There are many algorithms used for monitoring and controlling electric vehicles. To begin with, the Kalman filter (KF) algorithm is adopted for vehicle body slip angle estimation, and the linear quadratic regulator is used to control the system states [21], [22]. The idea is then extended in [2], where they are designed a robust  $H_\infty$  observer for an electric vehicle based on the lateral dynamic and measurements of yaw rate. Moreover, the extended KF and unscented KF algorithms for electric vehicle monitoring are presented in [23] and [24]. In order to estimate the vehicle position and shaft torque, the Luenberger observer is designed and verified in [25]. Considering the cyber attack, the cyber-physical system state estimation algorithm is developed in [26]–[28], but no optimal control algorithm is designed.

Moreover, the KF and Chi-squared detector-based trusted algorithm is designed for autonomous vehicle systems [29]. Additionally, the KF with a watermarking approach is proposed to detect the cyber attacks in [30]. Likewise, the neural network and decision tree-based cyber-attack protection schemes for resource-constrained vehicle systems are designed in [31] and [32]. In addition, the mixed-integer linear programming-based optimization approach is developed for minimizing vehicle security risks [33]. Currently, the transport layer security and effective handshaking schemes are the possible solutions for protecting vehicle infrastructures, IoT mobiles, and wireless terminals [34]. Based on the information gathering interval and historical LEGO data, a trial and error approach is proposed for resilient cyber attacks [35]. There is a little effort for developing an effective IoT-based vehicle state estimation algorithm considering cyber attacks. Specifically, there is no optimal gain and error covariance closed-form expressions considering cyber attacks in the IoT-based electric vehicle domain.

Furthermore, the steering actuator fault detection for an electric vehicle is designed in [36]. In order to control the vehicle speed, the Takagi–Sugeno control technique together with the Lyapunov stability approach is designed in [37]. Moreover, the Takagi–Sugeno observer is then designed to simultaneously estimate the vehicle steering and sideslip angles [38]. In addition, a nested proportional–integral–derivative (PID) steering control for lane keeping in vision-based autonomous vehicles is developed in [39]. Afterward, a robust gain-scheduled  $H_\infty$  controller for lateral stability control of electric vehicles is developed in [40]. Finally, a combination of automatic lane-keeping and driver's steering for electric vehicles through a two-degrees-of-freedom control strategy is proposed in [41]. To the best of our knowledge, there is little research on semidefinite programming-based optimal control algorithms for electric vehicle systems.

## B. Main Contributions

This article proposes state estimation and control algorithms for autonomous electric vehicles considering cyber attacks in

communication channels. The main contributions of this article are summarized as follows.

- 1) The interaction between the vehicle dynamics and the vision system are modeled by a state-space framework where the IoT-enabled smart sensors are deployed to obtain state information. The sensing information is transmitted to the control center over an unreliable communication network where attacks occur.
- 2) Based on the mean square error between the true and estimated system states, an optimal estimation algorithm is proposed to know and visualize the vehicle states from the received signals.
- 3) A semidefinite programming-based optimal feedback control algorithm is designed to stabilize the vehicle states. The feedback gain is obtained through the convex optimization process, and the designed gain is used to properly regulate the system states.
- 4) The numerical simulation results show that the proposed algorithm provides significant performance improvement compared with the existing method.

*Organizations:* The rest of this article is organized as follows. The problem statement is presented in Section II, which follows the vehicle state-space representation. The state estimation and control algorithms are developed in Sections IV and V, respectively. Finally, the simulation results and conclusion are presented in Sections VI and VII, respectively.

*Notations:* Boldface uppercase and lowercase letters are used to represent matrices and vectors, respectively. Superscript  $\mathbf{x}'$  denotes the transpose of  $\mathbf{x}$ ,  $E(\cdot)$  denotes the expectation operator, and  $\mathbf{I}$  denotes the identity matrix.

## II. PROBLEM STATEMENT

It is worth mentioning that the vehicle state estimation process is highly depended on the measurement accuracy and sensor precision. Basically, the measurement information is obtained by installed sensors, which are vulnerable to malfunction and cyber attacks [17], [18]. This raises safety and national security concerns which may lead to financial losses, travel, and social problems [19], [20]. Overall, the attack detection and minimization is one of the major challenges in the IoT-based electric vehicle to guarantee the resilient operation after taking appropriate actions. Considering the aforementioned challenges, the problem of interests in this article is: when the IoT sensing information is under cyber attacks what is the optimal vehicle state estimation algorithm that can tolerate cyber attacks, and what is the optimal control scheme to regulate the system states. This article addresses the aforementioned questions after developing the optimal state estimation and feedback control algorithms for autonomous electric vehicles using the IoT communication network considering false data injection attacks. The attackers inject this malicious information into the targeted network to mislead the control center. For developing algorithms, the vehicle model with on board vision system is first represented by a state-space framework in the following section.



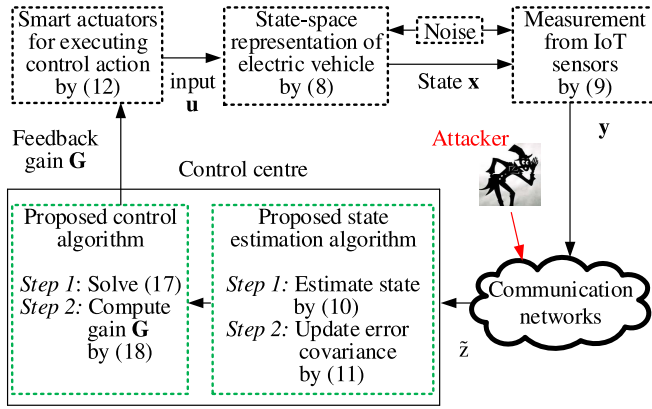


Fig. 3. Proposed IoT communication systems and algorithms.

environmentalist, and transport industry [1]. Due to environmental awareness and mitigate the global warming at an acceptable level, many people use battery powered or plug-in-electric vehicle instead of burning fossil fuels in transportation. It is believed that the IoT-based electric vehicle will be a part of a green, clean, and sustainable smart city. Basically, the intelligent transportation system is enhancing driving safety for automated vehicles. It provides services, such as automated vehicle tracking, smart fare, smart parking, and real-time traffic information [1], [2], [43]. For providing these services, the IoT sensors and communication infrastructure are the potential schemes. In order to sense and monitor the electric vehicle, the system operators deploy a set of IoT-enabled smart sensors whose measurements are described by

$$\mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{v}_k \quad (9)$$

where  $\mathbf{y}$  is the observation information,  $\mathbf{C}$  is the sensing matrix, and  $\mathbf{v}$  is the measurement noise with covariance matrix  $\mathbf{R}$ . The sensor locally processes the raw measurements, and the measurement innovation  $\mathbf{z}_k = \mathbf{y}_k - \mathbf{C}\hat{\mathbf{x}}_k^-$  ( $\hat{\mathbf{x}}_k^-$  is the *a priori* state information) is transmitted through the channel where attacks occur as shown in Fig. 3. The manipulated information is  $\tilde{\mathbf{z}}_k = \mathbf{T}_k\mathbf{z}_k + \mathbf{a}_k$ , where  $\mathbf{T}_k$  is the attacker matrix and  $\mathbf{a}_k$  is the channel noise. The attackers inject malicious information into the targeted network to mislead the control center. Based on the received information, the state estimation algorithm is designed to visualize the vehicle states while the control algorithm is used to regulate and stabilize the system states. Technically, the smart actuator executes the control action  $\mathbf{u}$ , which is described in the state-space model and Fig. 3.

#### IV. PROPOSED STATE ESTIMATION ALGORITHM

Based on the mean square error principle, the optimal state estimation algorithm is derived to know and visualize the vehicle states. For a given state-space framework in (8) and measurement in (9), the system state estimation is developed by using the following theorem.

*Theorem 1:* The state prediction and *a posteriori* estimation are give by

$$\tilde{\mathbf{x}}_k^- = \mathbf{A}_d\tilde{\mathbf{x}}_{k-1}, \quad \tilde{\mathbf{x}}_k = \tilde{\mathbf{x}}_k^- + \mathbf{K}\tilde{\mathbf{z}}_k. \quad (10)$$

Here,  $\tilde{\mathbf{x}}_{k-1}$  and  $\tilde{\mathbf{x}}_k$  are the *a priori* and *a posteriori* estimated states. The predicted and updated error covariances are given by [43]

$$\begin{aligned} \tilde{\mathbf{P}}_k^- &= \mathbf{A}_d\tilde{\mathbf{P}}_{k-1}\mathbf{A}_d' + \mathbf{Q} \\ \tilde{\mathbf{P}}_k &= \tilde{\mathbf{P}}_k^- + \tilde{\mathbf{P}}_k^-\left(\tilde{\mathbf{P}}_k^- - \tilde{\mathbf{T}}_k'\tilde{\mathbf{P}}_k^- - \tilde{\mathbf{P}}_k^-\tilde{\mathbf{T}}_k\right)\mathbf{C}\tilde{\mathbf{P}}. \end{aligned} \quad (11)$$

Here,  $\tilde{\mathbf{P}}_{k-1}$  is the *a priori* estimation error covariance and  $\tilde{\mathbf{P}} = (\mathbf{C}\mathbf{P}\mathbf{C}' + \mathbf{R})^{-1}$ . The optimal gain under steady-state condition is  $\mathbf{K} = \lim_{k \rightarrow \infty} \mathbf{K}_k = \tilde{\mathbf{P}}\mathbf{C}'(\mathbf{C}\tilde{\mathbf{P}}\mathbf{C}' + \mathbf{R})^{-1}$  with  $\tilde{\mathbf{P}} = \lim_{k \rightarrow \infty} \tilde{\mathbf{P}}_k$  and  $\tilde{\mathbf{P}}_0 = \tilde{\mathbf{P}}$ . The gain  $\mathbf{K}$  minimizes the error dynamic  $\tilde{\mathbf{z}}$  lead to an accurate estimated vehicle state over time. The aforementioned state estimation process is described in Fig. 3. The proof is derived in the Appendix.

After visualizing the vehicle states by estimation approach, the proposed control algorithm is designed to regulate the system states.

#### V. PROPOSED CONTROL ALGORITHM

In order to control the vehicle states, the optimal control algorithm is designed based on the semidefinite programming approach. According to the separation principle, the feedback control law is defined

$$\mathbf{u}_k = \mathbf{G}\mathbf{x}_k. \quad (12)$$

Here,  $\mathbf{G}$  is the feedback gain to be designed as shown in Fig. 3. The actuator executes the control action.

The closed-loop system is described as follows:

$$\mathbf{x}_{k+1} = (\mathbf{A}_d + \mathbf{B}_d\mathbf{G})\mathbf{x}_k + \mathbf{n}_k. \quad (13)$$

Inspired by the bounded real lemma without noise, consider the following optimization problem to find the optimal gain  $\mathbf{G}$ :

$$\begin{aligned} &\text{minimise } \xi \\ &\text{subject to } \mathbf{A}_{cl}'\mathbf{P}\mathbf{A}_{cl} - \mathbf{P} + \xi < \mathbf{0}, \mathbf{P} > \mathbf{0} \end{aligned} \quad (14)$$

where  $\xi > 0$  is the semidefinite programming variable which minimizes the estimator error covariance,  $\mathbf{P} > \mathbf{0}$  is a symmetric positive-definite matrix, and  $\mathbf{A}_{cl} = \mathbf{A}_d + \mathbf{B}_d\mathbf{G}$  is the closed-loop state matrix. Let us define  $\mathbf{X} = \mathbf{P}^{-1}$ , then the above inequality can be transformed into the following form:

$$\begin{aligned} &(\mathbf{A}_d + \mathbf{B}_d\mathbf{G})'\mathbf{X}^{-1}(\mathbf{A}_d + \mathbf{B}_d\mathbf{G}) - \mathbf{X}^{-1} + \xi < \mathbf{0} \\ &\mathbf{X}(\mathbf{A}_d + \mathbf{B}_d\mathbf{G})'\mathbf{X}^{-1}(\mathbf{A}_d + \mathbf{B}_d\mathbf{G})\mathbf{X} - \mathbf{X} + \xi\mathbf{X}\mathbf{X} < \mathbf{0}. \end{aligned} \quad (15)$$

Applying Schur's complement to (15) yields

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

In order to solve the above inequality using the linear matrix inequality (LMI) approach, let us define  $\mathbf{S} = \mathbf{G}\mathbf{X}$ , consequently, the above inequality can be written as follows:

$$\begin{bmatrix} -\mathbf{X} & \mathbf{X}\mathbf{A}_d' + \mathbf{S}'\mathbf{B}_d' & \mathbf{X} \\ (\mathbf{X}\mathbf{A}_d' + \mathbf{S}'\mathbf{B}_d')' & -\mathbf{X} & \mathbf{0} \\ \mathbf{X} & \mathbf{0} & -\xi\mathbf{I} \end{bmatrix} < \mathbf{0}. \quad (17)$$

TABLE I  
SIMULATION PARAMETERS USING MATLAB AND YALMIP

Symbols	Values	Symbols	Values
$m$	380 kg	$l_f$	0.8 m
$l_r$	0.6 m	$d_r$	0.82 m
$r$	0.22 m	$C_f$	6000 N/rad
$C_r$	6000 N/rad	$\mathbf{Q}$	$0.0005 \cdot \mathbf{I}$
$T$	0.001 sec	$\mathbf{R}$	$0.05 \cdot \mathbf{I}$

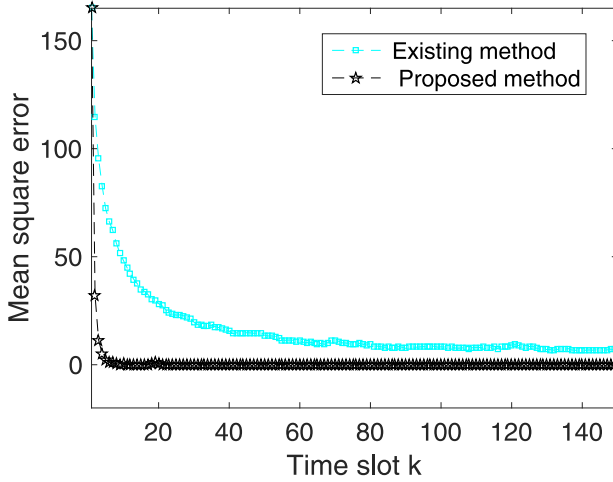


Fig. 4. Comparison of mean square error without sensor faults.

This is an LMI in the variables  $\mathbf{X}$  and  $\mathbf{S}$ . After solving (17), one can get  $\mathbf{X}$  and  $\mathbf{S}$ . Finally, the optimal gain is determined by

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

It can be effectively and efficiently solved by YALMIP software. The performance of the proposed method is analyzed in the next section.

## VI. SIMULATION RESULTS AND DISCUSSIONS

The whole simulation process is described in Fig. 3. It can be seen that after effectively representing the vehicle and IoT-sensing model, the proposed estimation and control algorithms are developed based on the received information. The state estimation and error covariance process is updated in each iteration using (10) and (11). After solving (17), the optimal feedback gain is determined by (18). The designed gain is used to properly regulate the system states. The simulation parameters are described in Table I [21]. The simulation is conducted with and without sensor faults conditions considering false data injection attack [4], [5].

During the time steps 10–20, the attackers are targeted the communication network, and it is considered that there is no sensor faults. From the simulation result in Fig. 4, it can be observed that the proposed algorithm outperforms the existing approach [27]. This is due to the fact that the proposed algorithm can effectively find the optimal solution to reduce the estimation errors while the existing method cannot find the optimal solution to properly track the system states [26]–[28]. When the estimation error dynamics are reduced, the true and estimated states are converged. To visualize, the vehicle

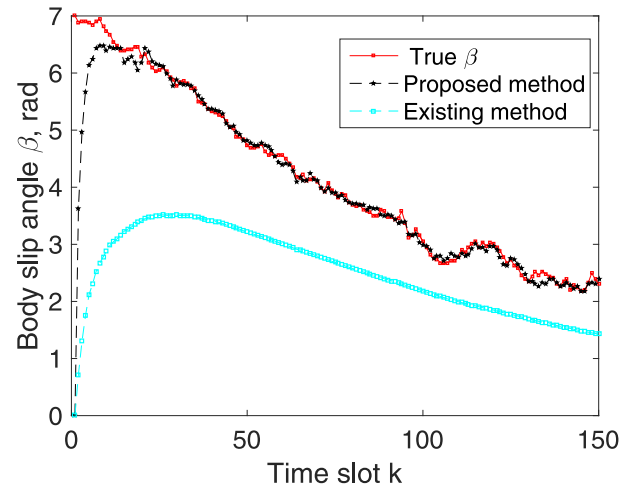


Fig. 5. Body slip angle  $\beta$  and its estimation without sensor faults.

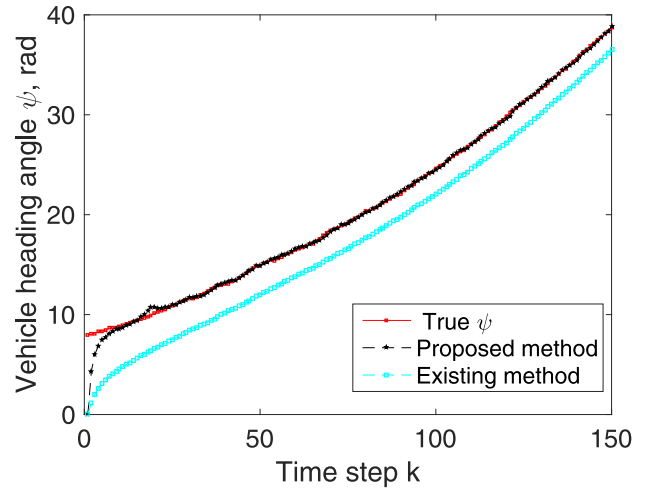


Fig. 6. Vehicle heading angle  $\psi$  and its estimation without sensor faults.

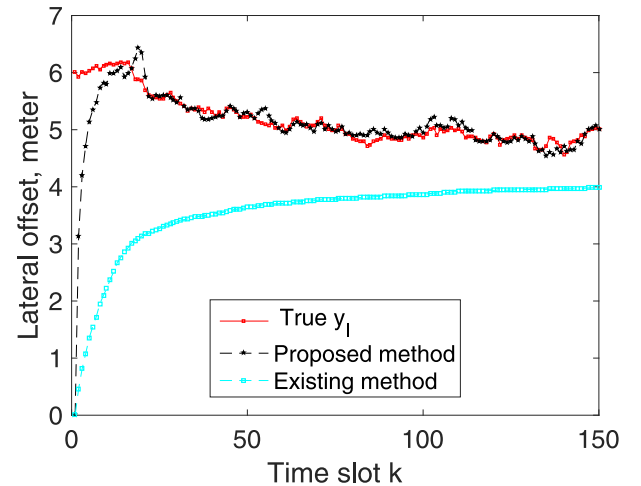


Fig. 7. Lateral offset  $y_l$  and its estimation without sensor faults.

dynamic state responses are plotted in Figs. 5–7. It can be seen that the proposed algorithm can able to properly estimate the system states. For instance, the vehicle slip angle  $\beta$  and its estimation result are presented in Fig. 5. Interestingly,

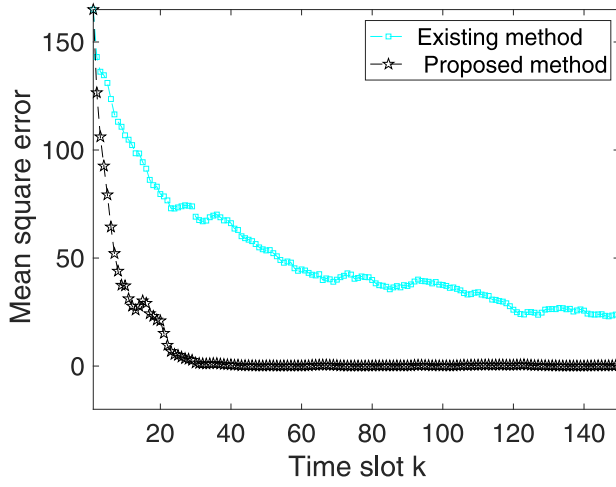


Fig. 8. Comparison of mean square error with sensor fault conditions.

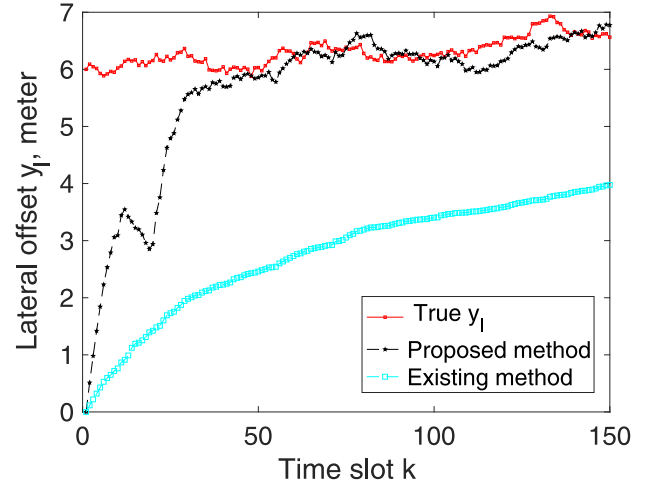
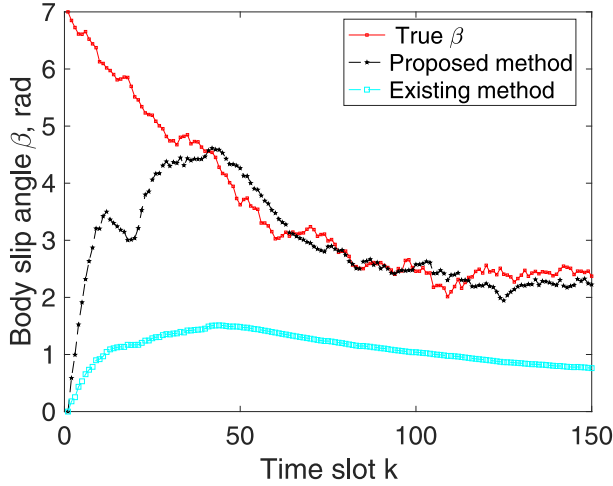
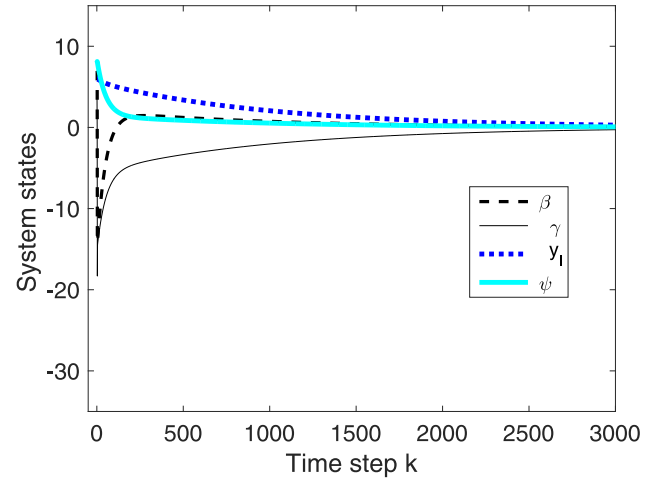
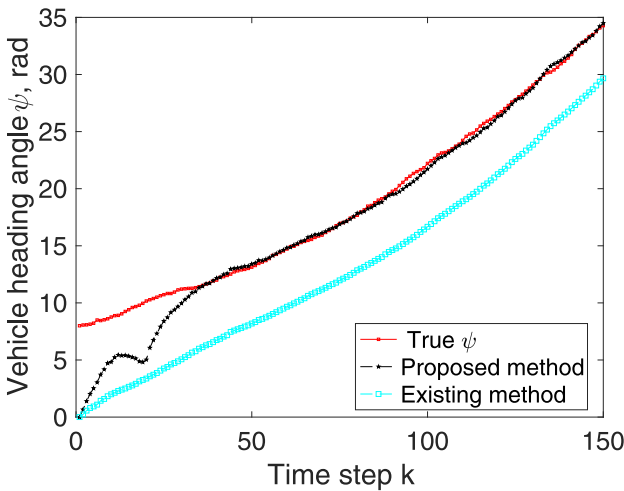

 Fig. 11. Lateral offset  $y_l$  and its estimation with sensor fault conditions.

 Fig. 9. Body slip angle  $\beta$  and its estimation with sensor fault conditions.


Fig. 12. Controlling the vehicle state trajectories.


 Fig. 10. Vehicle heading angle  $\psi$  and its estimation with sensor fault conditions.

the proposed algorithm requires around 22 iterations (time step  $k \times \text{sampling time } T = 0.022 \text{ s}$ ) to track system state while the existing method requires more than 150 iterations

( $k \times T = 0.15 \text{ s}$ ). The other vehicle states have similar kinds of estimation accuracy.

Sometimes, the sensing elements cannot sense the system states due to sensor faults and environmental conditions. Under sensor fault and cyber attack conditions, the mean square error between the true and estimated system states is shown in Fig. 8. Moreover, the system state responses versus time steps are presented in Figs. 9–11. It can be observed that the proposed method outperforms the aforementioned existing approach. It is also observed that under sensor fault and cyber attack conditions, the proposed method requires more time compared to fault-free condition as expected.

Generally speaking, the function of the control algorithm is to regulate the system states within a short period of time. The performance of the proposed control algorithm is illustrated in Fig. 12. After applying the proposed method, it can be seen that the developed approach can able to properly regulate the system states within 1600 iterations ( $k \times T = 1.6 \text{ s}$ ). Note that this stabilization time frame is less than the standard time 3 s [25]. This is due to the fact that the proposed controller can find the optimal feedback gain to stabilize the system states.



## VII. CONCLUSION

This article proposed optimal state estimation and control algorithms for monitoring and controlling the IoT-based electric vehicle under cyber attacks. After expressing the vehicle dynamic with onboard vision system into a state-space framework, the IoT-embedded smart sensors were used to sense the system states. The attacks occurred in a communication channel during the transmission of information to the control center. Based on the mean square error principle and semidefinite programming approaches, the proposed algorithms were designed. The simulation results show that the proposed estimation and control algorithms can properly estimate and stabilize the system states within a short period of time. Therefore, this article is valuable for designing the autonomous vehicle systems. The effectiveness of the proposed approaches will be experimentally verified in the future.

## APPENDIX PROOF OF THEOREM 1

For designing the state estimation algorithm, we assume that the control input  $\mathbf{u}_k$  is known [26], [43], so it is not considered as it cancels in the estimation process. Using (10), the *a priori* and *a posteriori* error dynamics are

$$\mathbf{x}_k - \tilde{\mathbf{x}}_k^- = \mathbf{A}_d(\mathbf{x}_{k-1} - \tilde{\mathbf{x}}_{k-1}^-) + \mathbf{n}_{k-1} \quad (19)$$

$$\mathbf{x}_k - \tilde{\mathbf{x}}_k = \mathbf{x}_k - \tilde{\mathbf{x}}_k^- - \mathbf{K}\tilde{\mathbf{z}}_k. \quad (20)$$

Using the mean square error principle, the above optimal gain  $\mathbf{K}_k$  is easy to obtain [43], [44]. The predicted error covariance is

$$\tilde{\mathbf{P}}_k^- = E[(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-)(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-)'] = \mathbf{A}_d\tilde{\mathbf{P}}_{k-1}\mathbf{A}_d' + \mathbf{Q}. \quad (21)$$

The *a posteriori* error covariance is expressed as follows [42], [43]:

$$\begin{aligned} \tilde{\mathbf{P}}_k &= E[(\mathbf{x}_k - \tilde{\mathbf{x}}_k)(\mathbf{x}_k - \tilde{\mathbf{x}}_k)'] = \tilde{\mathbf{P}}_k^- + \mathbf{K}(\mathbf{C}\tilde{\mathbf{P}}_k^- + \mathbf{R})\mathbf{K}' \\ &\quad - E[(\mathbf{x}_k - \tilde{\mathbf{x}}_k)\tilde{\mathbf{z}}_k'\mathbf{K}'] - [\mathbf{K}\tilde{\mathbf{z}}_k(\mathbf{x}_k - \tilde{\mathbf{x}}_k)']. \end{aligned} \quad (22)$$

For steady-state case, we assume that  $\tilde{\mathbf{x}}_0^- = \hat{\mathbf{x}}_0^-$  and  $\tilde{\mathbf{P}}_0 = E[(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-)(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-)] = \bar{\mathbf{P}}$ . Under this assumption and using (19), the term  $\mathbf{x}_k - \tilde{\mathbf{x}}_k^-$  in (22) is expressed as follows [42], [43]:

$$\begin{aligned} \mathbf{x}_k - \tilde{\mathbf{x}}_k^- &= \mathbf{A}_d\mathbf{x}_{k-1} + \mathbf{n}_{k-1} - \mathbf{A}_d(\tilde{\mathbf{x}}_{k-1}^- + \mathbf{K}\tilde{\mathbf{z}}_{k-1}) \\ &= \mathbf{A}_d^k\mathbf{x}_0 + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{n}_{k-1-l} - \mathbf{A}_d^k\tilde{\mathbf{x}}_0^- - \sum_{l=0}^{k-1}\mathbf{A}_d^{l+1}\mathbf{K}\tilde{\mathbf{z}}_{k-1-l}^- \\ &= \mathbf{A}_d^k(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-) + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{n}_{k-1-l} - \sum_{l=0}^{k-1}\mathbf{A}_d^{l+1}\mathbf{K}\tilde{\mathbf{z}}_{k-1-l}^-. \end{aligned}$$

Under the assumption,  $\mathbf{x}_k - \hat{\mathbf{x}}_k^-$  can be written as

$$\begin{aligned} \mathbf{x}_k - \hat{\mathbf{x}}_k^- &= \mathbf{A}_d\mathbf{x}_{k-1} + \mathbf{n}_{k-1} - \mathbf{A}_d(\hat{\mathbf{x}}_{k-1}^- + \mathbf{K}\mathbf{z}_{k-1}) \\ &= \mathbf{A}_d\mathbf{x}_{k-1} + \mathbf{n}_{k-1} - \mathbf{A}_d[\hat{\mathbf{x}}_{k-1}^- + \mathbf{K}\{\mathbf{C}(\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^-) + \mathbf{v}_{k-1}\}] \\ &= \mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})(\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^-) + \mathbf{n}_{k-1} - \mathbf{A}_d\mathbf{K}\mathbf{v}_{k-1}. \end{aligned}$$

Using the above information, the term  $\tilde{\mathbf{z}}_k = \mathbf{T}_k\mathbf{z}_k + \mathbf{a}_k$  can be written as [42], [43]

$$\begin{aligned} \tilde{\mathbf{z}}_k &= \mathbf{T}_k\mathbf{z}_k + \mathbf{a}_k = \mathbf{T}_k\mathbf{C}(\mathbf{x}_k - \hat{\mathbf{x}}_k^-) + \mathbf{T}_k\mathbf{v}_k + \mathbf{a}_k \\ &= \mathbf{T}_k\mathbf{C}\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})(\mathbf{x}_{k-1} - \hat{\mathbf{x}}_{k-1}^-) + \mathbf{T}_k\mathbf{C}\mathbf{w}_{k-1} \\ &\quad - \mathbf{T}_k\mathbf{C}\mathbf{A}_d\mathbf{K}\mathbf{v}_{k-1} + \mathbf{T}_k\mathbf{v}_k + \mathbf{a}_k \\ &= \mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^k(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-) \\ &\quad + \sum_{l=0}^{k-1}\mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^l\mathbf{w}_{k-1-l} + \mathbf{V}. \end{aligned} \quad (23)$$

Here, the noisy term  $\mathbf{V} = \mathbf{T}_k\mathbf{v}_k + \mathbf{a}_k - \sum_{l=0}^{k-1}\mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^l\mathbf{A}_d\mathbf{K}\mathbf{v}_{k-1-l}$  and  $E(\mathbf{V}) = \mathbf{0}$ .  $\tilde{\mathbf{z}}_k$  is the independent identically distributed Gaussian distribution, so orthogonality  $E(\tilde{\mathbf{z}}_i\tilde{\mathbf{z}}_j') = \mathbf{0}$ ,  $\forall i \neq j$ , and the third term of (22) can be expressed as follows [42], [43]:

$$\begin{aligned} &E[(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-)\tilde{\mathbf{z}}_k'\mathbf{K}'] \\ &= E\left[\left\{\mathbf{A}_d^k(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-) + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{n}_{k-1-l}\right\}\left\{\mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^k\right.\right. \\ &\quad \times \left.\left.(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-) + \sum_{l=0}^{k-1}\mathbf{T}_k\mathbf{C}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^l\mathbf{w}_{k-1-l}\right\}\mathbf{K}'\right] \\ &= \left\{\mathbf{A}_d^kE[(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-)(\mathbf{x}_0 - \hat{\mathbf{x}}_0^-)'][(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d']^k + \sum_{l=0}^{k-1}\mathbf{A}_d^lE\right. \\ &\quad \times \left.(\mathbf{n}_{k-1-l}\mathbf{n}_{k-1-l}')[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d']^l\right\}\mathbf{C}'\mathbf{T}_k'\mathbf{K}' \\ &= \left\{\mathbf{A}_d^k\bar{\mathbf{P}}[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d']^k + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{Q}[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d']^l\right\}\mathbf{C}'\mathbf{T}_k'\mathbf{K}' \\ &= \bar{\mathbf{P}}\mathbf{C}'\mathbf{T}_k'\mathbf{K}'. \end{aligned} \quad (24)$$

Here,  $\bar{\mathbf{P}}$  is the positive semidefinite matrix which is the composition function of Lyapunov  $h(\mathbf{X})$  [43] and Riccati operator  $g(\mathbf{X})$ , i.e.,

$$\begin{aligned} \bar{\mathbf{P}} &= (h \circ g)(\bar{\mathbf{P}}) \\ &= [\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^k\bar{\mathbf{P}}(\mathbf{A}_d')^k + \sum_{l=0}^{k-1}[\mathbf{A}_d(\mathbf{I} - \mathbf{K}\mathbf{C})]^l\mathbf{Q}(\mathbf{A}_d')^l \\ &= \mathbf{A}_d^k\bar{\mathbf{P}}[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d']^k + \sum_{l=0}^{k-1}\mathbf{A}_d^l\mathbf{Q}[(\mathbf{I} - \mathbf{K}\mathbf{C})'\mathbf{A}_d']^l. \end{aligned} \quad (25)$$

Similarly, the fourth term of (22) can be expressed as follows [43]:

$$E[\mathbf{K}\tilde{\mathbf{z}}_k(\mathbf{x}_k - \tilde{\mathbf{x}}_k^-)'] = \mathbf{K}\mathbf{T}_k\mathbf{C}\bar{\mathbf{P}}. \quad (26)$$

Substituting (24) and (26) into (22) yields  $\tilde{\mathbf{P}}_k$  in Theorem 1.

## REFERENCES

- [1] 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," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1575–1587, Jun. 2018.
- [2] H. Zhang, G. Zhang, and J. Wang, "Sideslip angle estimation of an electric ground vehicle via finite-frequency  $H_\infty$  approach," *IEEE Trans. Transport. Electric.*, vol. 2, no. 2, pp. 200–209, Jun. 2016.

- [3] A. Djenna and D. E. Saïdouni, "Cyber attacks classification in IoT-based-healthcare infrastructure," in *Proc. Cyber Security Netw. Conf.*, 2018, pp. 1–4.
- [4] Y. Mo, R. Chabukswar, and B. Sinopoli, "Detecting integrity attacks on SCADA systems," *IEEE Trans. Control Syst. Technol.*, vol. 22, no. 4, pp. 1396–1407, Jul. 2014.
- [5] A. Nourian and S. Madnick, "A systems theoretic approach to the security threats in cyber physical systems applied to stuxnet," *IEEE Trans. Depend. Secure Comput.*, vol. 15, no. 1, pp. 2–13, Jan./Feb. 2018.
- [6] M. T. Khan, D. Serpanos, and H. Shrobe, "ARMET: Behavior-based secure and resilient industrial control systems," *Proc. IEEE*, vol. 106, no. 1, pp. 129–143, Jan. 2018.
- [7] M. Marjani *et al.*, "Big IoT data analytics: Architecture, opportunities, and open research challenges," *IEEE Access*, vol. 5, pp. 5247–5261, 2017.
- [8] C. A. Tokognon, B. Gao, G. Y. Tian, and Y. Yan, "Structural health monitoring framework based on Internet of Things: A survey," *IEEE Internet Things J.*, vol. 4, no. 3, pp. 619–635, Jun. 2017.
- [9] J. Pan and J. McElhannon, "Future edge cloud and edge computing for Internet of Things applications," *IEEE Internet Things J.*, vol. 5, no. 1, pp. 439–449, Feb. 2018.
- [10] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.
- [11] 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.
- [12] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.
- [13] A. Singh and M. Singh, "An empirical study on automotive cyber attacks," in *Proc. World Forum Internet Things*, 2018, pp. 47–50.
- [14] A. Bandekar and A. Y. Javaid, "Cyber-attack mitigation and impact analysis for low-power IoT devices," in *Proc. Annu. Int. Conf. Cyber Technol. Autom. Control Intell. Syst.*, 2017, pp. 1631–1636.
- [15] M. A. Razaque, 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.
- [16] 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.
- [17] X. Yang, P. Zhao, X. Zhang, J. Lin, and W. Yu, "Toward a Gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 147–161, Feb. 2017.
- [18] A. S. Musleh, H. M. Khalid, S. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, Mar. 2019.
- [19] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017.
- [20] M. N. Kurt, Y. Yilmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.
- [21] 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.
- [22] K. Nam, S. Oh, H. Fujimoto, and Y. Hori, "Estimation of sideslip and roll angles of electric vehicles using lateral tire force sensors through RLS and Kalman filter approaches," *IEEE Trans. Ind. Electron.*, vol. 60, no. 3, pp. 988–1000, Mar. 2013.
- [23] W. Cheng, S. Chuanxue, and L. Jianhua, "Research on key state parameters estimation of electric vehicle ESP based on multi-sensor," in *Proc. Int. Conf. Instrum. Meas. Comput. Commun. Control*, 2015, pp. 29–32.
- [24] 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.
- [25] 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.
- [26] M. M. Rana, "Attack resilient wireless sensor networks for smart electric vehicles," *IEEE Sensors Lett.*, vol. 1, no. 2, pp. 1–4, Apr. 2017.
- [27] A. Ahmed, U. M. Al-Saggaf, and M. Moinuddin, "State space least mean fourth algorithm for state estimation of synchronous motor," *Asian J. Eng. Sci. Technol.*, vol. 4, no. 1, pp. 9–12, 2014.
- [28] M. B. Malik and M. Salman, "State-space least mean square," *Digit. Signal Process.*, vol. 18, no. 3, pp. 334–345, 2008.
- [29] 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.
- [30] 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.
- [31] A. Sargolzaei, C. D. Crane, A. Abbaspour, and S. Noei, "A machine learning approach for fault detection in vehicular cyber-physical systems," in *Proc. Int. Conf. Mach. Learn. Appl.*, 2016, pp. 636–640.
- [32] T. P. Vuong, G. Loukas, D. Gan, and A. Bezemskij, "Decision tree-based detection of denial of service and command injection attacks on robotic vehicles," in *Proc. Int. Workshop Inf. Forensics Security*, 2015, pp. 1–6.
- [33] S. Mousavian, M. Erol-Kantarci, L. Wu, and T. Ortmeyer, "A risk-based optimization model for electric vehicle infrastructure response to cyber attacks," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6160–6169, Nov. 2018.
- [34] J. Cai *et al.*, "A handshake protocol with unbalanced cost for wireless updating," *IEEE Access*, vol. 6, pp. 18570–18581, 2018.
- [35] 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.
- [36] 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.
- [37] 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.
- [38] 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.
- [39] 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.
- [40] 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.
- [41] V. Cerone, M. Milanese, and D. Regruto, "Combined automatic lane-keeping and driver's steering through a 2-DOF control strategy," *IEEE Trans. Control Syst. Technol.*, vol. 17, no. 1, pp. 135–142, Jan. 2009.
- [42] M. M. Rana and R. Bo, "IoT-based improved human motion estimations method under cyber attacks," *IEEE Internet Things J.*, to be published.
- [43] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Optimal linear cyber-attack on remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 4–13, Mar. 2017.
- [44] D. Simon, *Optimal State Estimation: Kalman, H Infinity, and Nonlinear Approaches*. Hoboken, NJ, USA: Wiley, 2006.