IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 August 2024, accepted 1 September 2024, date of publication 4 September 2024, date of current version 13 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3454560

RESEARCH ARTICLE

Neural Network-Based Cyber-Threat Detection Strategy in Four Motor-Drive Autonomous Electric Vehicles

DOUGLAS G. SCRUGGS[1], LAXMAN TIMILSINA[2], (Member, IEEE), BEHNAZ PAPARI[1,2], (Senior Member, IEEE), ALI ARSALAN[1], (Graduate Student Member, IEEE), GRACE MURIITHI[1], (Graduate Student Member, IEEE), GOKHAN OZKAN[2,3], (Senior Member, IEEE), AND CHRISTOPHER S. EDRINGTON[2], (Senior Member, IEEE)

[1]Secure Energy and Automation Laboratory (SEAL), Department of Automotive Engineering, Clemson University, Greenville, SC 29607, USA
[2]Real-Time COntrol and Optimization Laboratory (RT-COOL), The Holcombe Department of Electrical and Computer Engineering, Clemson University, Clemson, SC 29634, USA
[3]Dominion Energy Innovation Center, Clemson University, North Charleston, SC 29405, USA

Corresponding author: Laxman Timilsina (ltimils@clemson.edu)

ABSTRACT Autonomous electric vehicles provide benefits to both drivers and the environment compared to conventional vehicles; however, they are burdened with an increase in potential pathways for cyber-attacks. Therefore, reliable cyber-security strategies for these vehicles must be pursued. This paper addresses this concern by implementing a threat detection strategy that utilizes an observer and a neural network. These tools monitor discrepancies between the vehicle's lateral metrics, which are produced via sensor data, neural network output, and an observer. Previous literature focuses on physics-based analytics to create the threat decision, but here, a data based approach is utilized. The vehicle used in this study is a four-motor-drive autonomous electric vehicle that is propelled with brushless DC motors. The motors are controlled by direct torque control. In this study, three forms of cyber-attacks are implemented. These include data integrity attacks, replay attacks, and denial-of-service attacks. A performance metric is also created, which indicates the data-driven approach outperforms the physics-based approaches. All modeling and simulation were conducted in the MATLAB/Simulink environment.

INDEX TERMS Electric vehicle (EV), lateral stability control system (LSCS), direct torque control (DTC), yaw rate, sideslip angle, cyberattack.

ACRONYM

DIA	Data Integrity Attack.
DL	Deep Learning.
DM	Detection Method.
DOS	Denial-of-Service.
DTC	Direct Torque Control
EV	Electric Vehicle.
FNN	Feed-Forward Neural Network.
HEV	Hybrid Electric Vehicle.
LQR	Linear Quadratic Regulator.
LSCS	Lateral Stability Control System.
LSTM	Long Short-Term Memory.
MPC	Model Predictive Control.
PID	Proportional–Integral–Derivative
V2G	Vehicle-to-Grid.

The associate editor coordinating the review of this manuscript and approving it for publication was Wei Xu.

I. INTRODUCTION

Electrified vehicles are increasingly preferred for transportation due to their ability to address significant environmental pollution and decrease reliance on petroleum products.

Despite the notable advantages of EVs, their widespread adoption is currently hindered by various challenges [1], [2]. A significant obstacle lies within the realm of cyber attacks [3]. As the number of electric vehicles (EVs) and autonomous vehicles become more prevalent, a paralleled increase in cyber threat targets occurs. This vulnerability is particularly pronounced when EVs are connected to charging substations or engaged in vehicle-to-grid (V2G) operations [4]. Study [5] provides insight into this arising issue. In [6], the authors argue for software and hardware security standards in autonomous vehicles to mitigate safety concerns. This point is emphasized by [7], where the authors point out the lack of security infrastructure concerning intelligent vehicles. Decentralized communication schemes are provided in [8], which reduces the probability of potential threats given vehicles are communicating with each other. With regards to the development of intelligent vehicles, the authors in [9] provide a process for vehicle development called cybersecurity and safety management system that incorporates standards ISO 26262 and ISO/SAE 21434. Malicious intent aimed at a vehicle's Lateral Stability Control System (LSCS) not only compromises the safety of the vehicle targeted but also puts all that is in the vehicle's surroundings in danger via proximity. Therefore, cyber-threat detection strategies that prove to be resilient, dependable, and timely must be pursued [10].

The authors in [11] investigate cyber-threat detection methods for cyber-attacks located in a vehicle's LSCS. A residual band is developed that monitors the actual, estimated, and targeted values used by the LSCS to detect the presence of an attack. This study builds upon the work in [11] by predicting current lateral values with a feed-forward neural network. In [12], a similar scheme is introduced that utilizes a long short-term memory (LSTM) architecture.

Vehicular lateral movements can be accomplished through adjustments to the vehicle's yaw rate and sideslip angle. Sensor information is typically used to monitor and control these values. While yaw-rate is an easily discerend value from a yaw-rate sensor, sideslip angle is more difficult to glean. In [13], it is seen that direct measurement of the signal is involved. Therefore, estimates are commonly made to describe the vehicle's sideslip angle. Similarly to what is seen in [14], the vehicle in this study determines the optimal yaw rate and sideslip angle for a vehicle through model predictive control (MPC). Here, the MPC is responsible for finding what lateral trajectory commands minimize the absolute difference between the target and actual lateral position. The reliability of MPC for yaw stability in four motor-drive vehicles is also seen in [14], where MPC is used to maintain stability under various circumstances. The authors of [15] demonstrate lateral and longitudinal stability control through the combination of nonlinear MPC and proportional–integral–derivative (PID) control. A sliding-mode control for yaw-moment is presented in [16], which also presents a method for estimating the sideslip angle of a vehicle. In addition to MPC utilized for yaw stability, optimal yaw metrics can also be determined by means of direct yaw control, as seen in [17] and [18]. In [17] and [18], calculations are deployed that stabilize the vehicle's lateral motions while completing driving maneuvers. Neural Networks have also been applied for yaw stability, as seen in [19].

Yaw control often develops a yaw-moment which can be used to determine appropriate torque values to be applied to each of the vehicle's wheels to complete a lateral motion. Most motor control schemes are designed to control the shaft speed of a motor and, therefore, do not reflect the needs of this problem. However, direct torque control (DTC) remedies this issue by directly controlling the output torque of the motor. In this study, the modeling scheme seen in [20] is implemented. A similar approach is seen in [21], which neglects the estimated flux angle value while still providing high-resolution torque control. The 4-pole, brushless-DC motor modeling for this simulation is governed by the equations seen in [22].

In recent times, cyber-threat detection in electric vehicles has been more heavily investigated. Recently, the authors of [23] developed electrical improvements for vehicle cyber-security concerning the vehicle's network, controller, and communication. In [24], a physics-guided machine-learning approach is used for this purpose. Here, the tracking accuracy of the qd currents in vehicle machines, as well as torque, are used as inputs for an LSTM. In [25], vulnerability is analyzed through velocity tracking error, energy efficiency and consumption, and acceleration transitions in the event of several forms of attack. The cyber-security of hybrid electric vehicles (HEV) has also been studied in the event of sophisticated cyber-attacks, as seen in [26]. This study investigates attacks related to the vehicle's energy management system, which can threaten the vehicle's battery capacity. Research has not only pursued cyber-security with respect to EVs on the road but also regarding EV charging. The study conducted in [27] investigates the cyber vulnerabilities seen in the electric grid and EVs as the deployment of EVs steadily increases. As seen in [28], the author addresses cyber-security concerns in smart charging infrastructure and provides insight for increasing security. In [29], the authors discuss the impact on EV batteries' state of charge in the event of different types of cyber-attacks while the vehicle is charging. Moreover, concerns regarding grid voltage and frequency are expressed in [30] in the event of a cyber-attack with the addition of new intelligent infrastructure. Cyber-attacks placed on a Navy ship are studied in [31]. Here the power system is distributed, and the power quality is observed for different attacks. Machine learning has been applied in [32] to predict attacks on EV charging stations. Artificial Intelligence is also applied in [33], where the authors apply an LSTM to detect an attack under various conditions. As discussed earlier, the prevalence of autonomous electrified transportation is increasing. Therefore, reliable schemes must be found for the sake of cyber security. To address the above-discussed issues, this paper proposes a novel neural network-based cyber-physical attack detection method for detecting cyber

threats in the vehicle's LSCS. The major contributions of this proposed work are given as follows:

- A methodology for realizing lateral vehicle movements by integrating the resolution of a MPC problem and employing a linear quadratic regulator for state tracking is proposed. Additionally, a motor control scheme is presented, tailored to address the requirements of the lateral stability control issue and achieve the specified torque commands.
- A neural network-based residual metric approach is proposed for vehicle state estimation and also for the purpose of cyber-security. Further, a performance comparison of multiple detection methods in the event of various forms of cyber-attacks is detailed.

The remainder of this paper is structured as follows. In Section II, the vehicle modeling, as well as the lateral and longitudinal control techniques for the vehicle, are presented. Section III describes the three types of attacks used against the LSCS in this study. The workings and modeling of the three cyber-threat detection schemes are presented in Section IV, and Section IV-D provides an in-depth analysis of the detection method's performances. The main conclusions drawn from the proposed work are given in Section VI.

II. MODELLING AND CONTROL OF ELECTRIC VEHICLE

The objective of this study's vehicle model is to complete a double-lane change maneuver for the vehicle. This is accomplished through three layers of control. These layers include an outer loop for path tracking, an inner loop for reference trajectory command tracking, and an inner loop for motor control. This procedure is very similar to that which is seen in [11]. Fig. 1 depicts the system's structure as well as the interactions between the control layers. The devil in Fig. 1 depicts the cyber-attack targets.

A. HUMAN DRIVER SYNTHESIZED BY MEANS OF MODEL PREDICTIVE CONTROL

If an EV's LSCS is placed under a cyberattack, its lateral path tracking capability becomes compromised. This means that the ordinary driving maneuvers a car driver uses would no longer provide a normal lateral response. However, the driver will notice trends in the vehicle's behavior and can adapt to the vehicle's new behavior. MPC is a well-suited control method for mimicking a human driver's intelligence.

The purpose of the MPC loop is to move the vehicle to a desired lateral location. It does this by assigning the optimal lateral movement commands to the system's LSCS. These commands include a reference yaw rate denoted as γ_{ref} and a reference sideslip angle denoted as β_{ref}. The MPC problem determines what values for yaw rate and sideslip angle would minimize the difference between the vehicle's current lateral position, denoted as S_y and its target lateral position, denoted as $S_{y,ref}$ for future time steps. Predicted lateral positions are found using (1) where V_x is longitudinal velocity, t_p is the time of the future horizon, and ϕ is the heading angle.

$$S_y(t+t_p) = (t_p - t) \times \Big(V_x \times \sin(\gamma(t_p) \times (t_p - t) + \phi(t)) + V_x \times \tan(\beta(t_p)) \times \cos(\gamma(t_p) \times (t_p - t) + \phi(t)) \Big) + S_y(t) \tag{1}$$

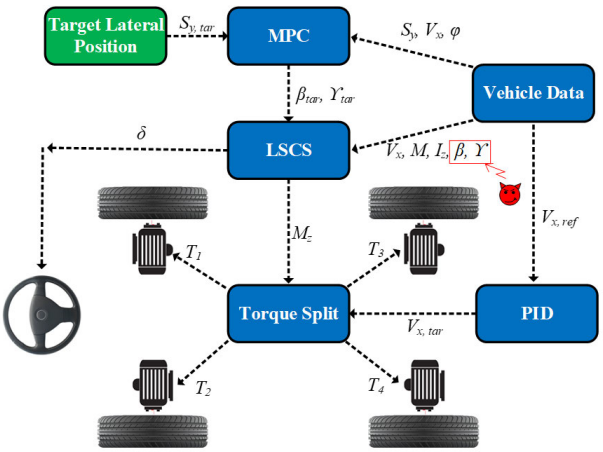


FIGURE 1. System diagram of interaction between various control layers in EV.

Once the predicted lateral position has been found, (2) is used to determine what values of β and γ bring the vehicle closest to the target location.

$$\min \int_t^{t_p} (S_y(t_p) - S_{y,ref}(t))^2 dt \tag{2}$$

B. LATERAL STABILITY CONTROL SYSTEM OF EV

The purpose of the LSCS is to bring the vehicle's yaw rate and sideslip angle to their target values determined by the MPC. By developing state space equations where yaw rate and sideslip are the system's states, and steering wheel angle denoted as δ, and additional yaw moment denoted as M_z as control inputs, a linear quadratic regulator (LQR), can be used to bring the states to the desired values.

Using the differential equations describing β and γ, the state matrix and input matrix for this system are created [5].

In equations (3a) and (3b), as shown at the bottom of the next page, C_y represents cornering stiffness, which is different for the front and rear axles. L_f is the distance from the front axle to the vehicle's center of mass, L_r is the distance from the rear axle to the vehicle's center of mass, I_z is the vehicle's moment of inertia, and m is the vehicle's mass.

$$\begin{bmatrix} \beta' \\ \gamma' \end{bmatrix} = A \begin{bmatrix} \beta \\ \gamma \end{bmatrix} + B \begin{bmatrix} \delta \\ M_z \end{bmatrix} \tag{4}$$

Equation (4) depicts the entire state space equation for the LSCS. As stated previously, an LQR is used to bring the vehicle's yaw rate and sideslip angle to the target values provided by the MPC. The LQR solves for the optimal gain matrix, K, that can be used to bring the LSCS's states to their desired values. In this equation, Q and R are tuned weighting

matrices. For this solution, the cross-term matrix N has been ignored.

The gain matrix is found using (5), where the gain matrix minimizes cost. Gain matrix K is found offline and is applied during simulation. Variable x in (5) indicates the difference between the target states solved through MPC and the actual states of the system. Therefore, in (5), x holds system's error which (5) aims to minimize.

$$J = \int_0^\infty \left(x^T Q_x + u^T R_u + N_u\right) dt \tag{5}$$

The inputs sent to the LSCS are then calculated using (6).

$$\begin{bmatrix} \delta \\ M_z \end{bmatrix} = -K \begin{bmatrix} \beta - \beta_{ref} \\ \gamma - \gamma_{ref} \end{bmatrix} \tag{6}$$

C. MOTOR TORQUE CONTROL FOR BLDC DRIVE SYSTEM

Two metrics are necessary to calculate the necessary output torque of each motor to fulfill a desired lateral movement. These metrics are the additional yaw moment found using the LQR, and the total torque demand, T_{dem}, found using longitudinal control. T_{dem} is found using (7), where r_w is the wheel radius, M is the mass of the vehicle, ρ_a is air density, A_f is the area of the vehicle's face, C_d is the coefficient of air resistance, θ is the slope of the road, and f is the coefficient of rolling resistance.

$$T_{dem} = r_w(Ma_r + \frac{1}{2}\rho_a A_f C_d v_x^2 + Mg[sin(\theta) + fcos(\theta)]) \tag{7}$$

PID control is used to bring the vehicle to its desired longitudinal speed. The PID's error signal is the difference between actual speed and target speed and uses this signal as an acceleration command in (7).

Consider the motor associated with the front left wheel to be motor 1, front right wheel motor 2, back left wheel motor 3, and back right wheel motor 4. The target torque demanded for motor 1 and motor 3 are given by (8a) and (8b), respectively.

$$T_{ref,1} = \frac{1}{4}T_{dem} - \Delta T_{ref,1} \tag{8a}$$

$$T_{ref,3} = \frac{1}{4}T_{dem} - \Delta T_{ref,3} \tag{8b}$$

The delta component of these equations is given by (9a) and (9b).

$$\Delta T_{ref,1} = \frac{L_f r_w}{(L_f + L_r)L_d} M_z \tag{9a}$$

$$\Delta T_{ref,3} = \frac{L_r r_w}{(L_f + L_r)L_d} M_z \tag{9b}$$

The output torque of motor 2 and motor 4 are given by (10a) and (10b).

$$T_{ref,2} = \frac{1}{4}T_{dem} - 2\Delta T_{ref,1} \tag{10a}$$

$$T_{ref,4} = \frac{1}{4}T_{dem} - 2\Delta T_{ref,3} \tag{10b}$$

Note that the total torque demand does not depict the sum of reference torques for each wheel in periods where the vehicle is making lateral movements. This is due to the reference torque demands being a function of the additional yaw-moment. When the vehicle is not making a lateral movement, the sum of reference torques is equal to the total torque demand since the additional yaw-moment is zero.

Since the nature of the lateral stability control problem involves controlling the torque applied at each of the wheels, the motor control method, DTC, is used. This method works by making an estimate of the machine's flux linkage magnitudes and the machine's electrical output torque. Both the flux linkage magnitude and output torque have the desired values. The desired torque magnitude is held constant while the torque estimate is made using the control scheme. If the estimated values fall above or below the desired values, an inverter switching sequence is executed to bring the estimated values closer to the desired values.

To determine the correct switching sequence, the electrical position of the machine must first be found by taking the magnitude of the q and d axis stator flux vectors in the synchronous reference frame. α is then found by taking the atan of these two vectors. From Fig. 2, we can see that there are 6 possible positions, each with a bandwidth of 60°.

After determining the electrical position of the machine, as well as the estimated torque and flux vector, the optimal voltage vector can be applied. The voltage vector is a function of the switch position in the inverter.

In this model, a 6-switch, 2-level inverter is used. For this control scheme, switches associated with the same phase

$$\mathbf{A} = \begin{bmatrix} -\frac{2 \times (C_{yf} + C_{yr})}{(V_x \times m)} & -\frac{2 \times ((L_f \times C_{yf}) - (L_r \times C_{yr}))}{(V_x^2 \times m)} \\ -\frac{2 \times ((L_f \times C_{yf}) - (L_r \times C_{yr}))}{(I_x)} & -\frac{2 \times ((L_f^2 \times C_{yf}) - (L_r^2 \times C_{yr}))}{(I_x \times V_x)} \end{bmatrix} \tag{3a}$$

$$\mathbf{B} = \begin{bmatrix} \frac{2 \times C_{yf}}{(V_x \times m)} & 0 \\ \frac{(2 \times C_{yf} \times L_f)}{(I_x)} & \frac{1}{I_x} \end{bmatrix} \tag{3b}$$

cannot be on at the same time. Therefore, there are 8 different switching sequences.

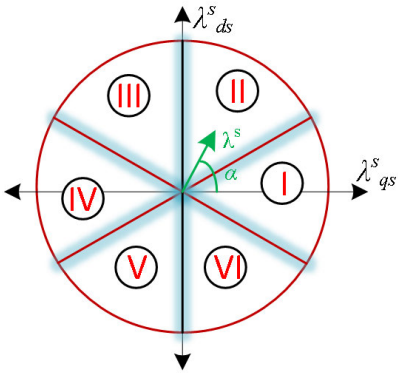


FIGURE 2. Graph of stator flux position sequences using DTC [12].

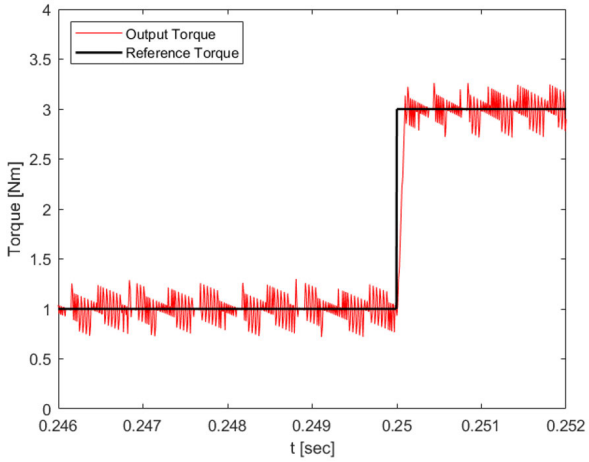


FIGURE 3. DTC step-response performance during step-response.

For this EV, four 3-phase brushless DC motors were used. Fig. 3 depicts a DC motor's response to an initial torque command of 1 $N-m$, followed by a 4 $N-m$ torque command. This shows how well-suited DTC is for this EV model. Vehicle specifications for this study are given in Table 1.

TABLE 1. Parameters of EV from (8)-(14).

Parameter	Value
r_w	0.3m
M	1575kg
ρ_a	1.225kg
I_s	4000 kg*m^2
L_r	1.6m
L_f	1.2m

III. MODELLING OF VARIOUS CYBER-ATTACKS

In this study, three types of cyber-attacks are used. These include data integrity attacks (DIAs), replay attacks, and Denial-of-Service (DOS). DIAs can be seen in the form of (11).

$$y_{atck} = vy + \epsilon \tag{11}$$

From (11), y_{atck} represents the signal sent to the LSCS, y represents the actual value of the signal, v represents a scaling value for the signal, and ϵ depicts a value summed with the scaled signal. DIAs are started at $t = 3$s and last until $t = 4$s.

Replay attacks can be seen as attacks that prevent the update of information to the system's LSCS and the MPC. Therefore, in the event of a replay attack, the metric under attack will be seen as the same value that occurred at the beginning of the attack. The intensity of the attack varies on the length of the attack. Each simulated replay attack begins at $t = 3.2$s and lasts for a variable amount of time.

DOS attacks affect how frequently a monitored signal is updated. In this study, DOS attacks are enacted by manipulating the time-step of a certain variable in the simulation while holding another monitored signal at the normal time step.

The vehicle's LSCS utilizes the vehicle's mass, moment of inertia, yaw rate, sideslip angle, and longitudinal cruising speed. Yaw rate and sideslip angle are the most dynamic signals and are therefore placed under attack.

It should be noted that this study is mainly concerned with detecting cyber-attacks that still provide the driver with enough control to complete the maneuver reasonably. Therefore, attacks leading to complete instability will not be considered since the vehicle is obviously under a cyber-attack in this scenario.

IV. MODELLING AND COMPARISON OF DETECTION STRATEGIES

In this study, three different attack detection strategies are used. While they are different, the fundamentals of the detection schemes are the same. Each scheme uses a residual metric that is a sum of the error between two values across 10-time steps. The values associated with this error metric concern the states of the LSCS, i.e., sideslip angle and yaw rate. A threshold of 0.0025 is used for each of the detection schemes.

A. COMPARISON BETWEEN ESTIMATED AND ACTUAL LATERAL METRICS

A comparison between actual and estimated values is made by first making an estimate of the system's yaw rate and sideslip angle. This is done by finding an observer gain L that will make the observer system converge to the actual states. Converging to the actual states is achieved by placing the poles of the system farther out in the left half-plane. The state matrices for the observer system have the form seen in (12a) – (12c).

$$\mathbf{A} = \begin{bmatrix} A-Bk & Bk \\ zero(size(A)) & A-LC \end{bmatrix} \tag{12a}$$

$$\mathbf{B} = \begin{bmatrix} B \\ zero(size(B)) \end{bmatrix} \tag{12b}$$

$$\mathbf{C} = \begin{bmatrix} C & zero(size(C)) \end{bmatrix} \tag{12c}$$

Now that an estimated value has been created, a residual metric comparing estimated states to actual states can be summed over 10-time steps. This is computed using (13), where β_{est} and γ_{est} are the estimated values of β and γ.

$$r_1 = \sum_{i=1}^{10} \left(\beta_i - \beta_{\text{est,i}}\right)^2 + \left(\gamma_i - \gamma_{\text{est,i}}\right)^2 \tag{13}$$

At the end of 10-time steps, the maximum residual value for those 10-time steps is saved, and the residual is set back to 0. These maximum residual values are used to create a residual array. For each set of 10-time steps, the residual array holds the same value, which is the maximum residual for those 10-time steps during normal operating conditions. If, during simulation, the residual during a set of 10-time steps surpasses the max residual associated with those same 10-time steps, it is believed that a cyber threat has been placed on the system, and a flag is raised.

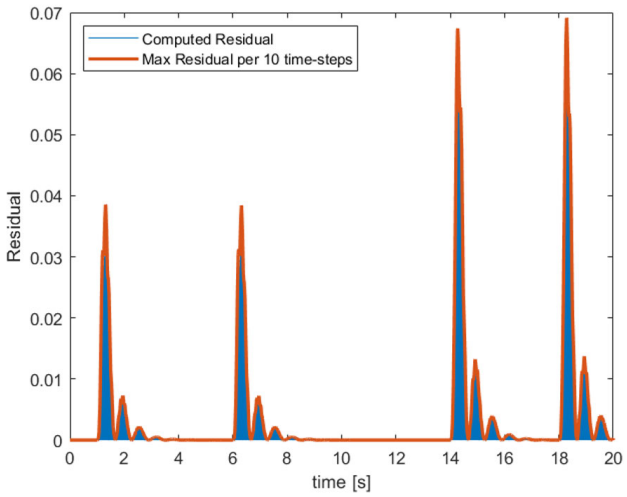


FIGURE 4. Residual metric for DM:1 [6].

Fig. 4 provides a visible explanation as to the scheme. In orange is the max residual per 10-time steps. This value is the same for every 10-time steps in the array. The simulated residual is seen in blue. It is continuously summed for 10-time steps and is then set back equal to 0 at the end of the tenth time step. The only way this metric comparing estimated to actual states can flag a security alert is by simulated residual growing above the orange band. For the remainder of this paper, for simplicity, the detection method will be represented as DM, and this particular detection strategy will be denoted as DM:1.

B. COMPARISON BETWEEN ESTIMATED AND TARGET LATERAL METRICS

The security metric comparing estimated and target values has a very similar methodology and execution.

$$r_2 = \sum_{i=1}^{10} \left(\beta_{\text{tar,i}} - \beta_{\text{est,i}}\right)^2 + \left(\gamma_{\text{tar,i}} - \gamma_{\text{est,i}}\right)^2 \tag{14}$$

Equation (14) depicts the residual calculation for this new metric. It is the same as (13), except the estimated value is being compared to the target value instead of the actual value.

Fig. 5 illustrates the residual band created using this equation. This residual band has larger peaks than the previous one. For the remainder of this paper, this detection strategy will be denoted as DM:2.

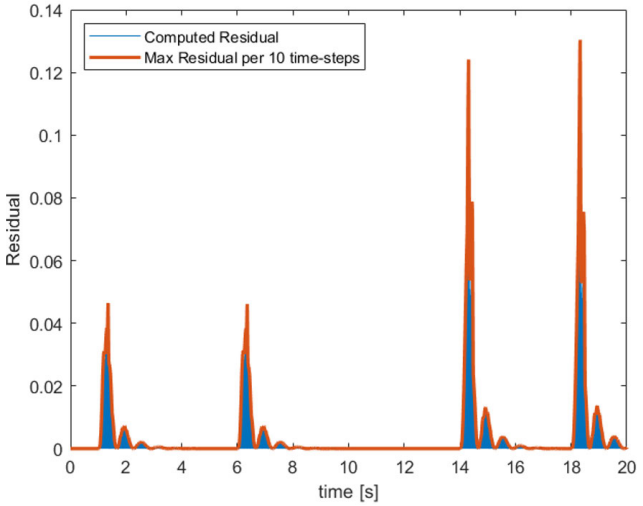


FIGURE 5. Residual metric for DM:2 [6].

C. COMPARISON BETWEEN ESTIMATED AND NEURAL NETWORK PREDICTIONS FOR LATERAL METRICS

A feed-forward neural network (FNN) was used for a similar purpose as the previous two metrics. The FNN takes on four inputs and produces two outputs. Fig. 6 depicts the structure of the FNN. Study [12] provides a similar method to accomplish this.

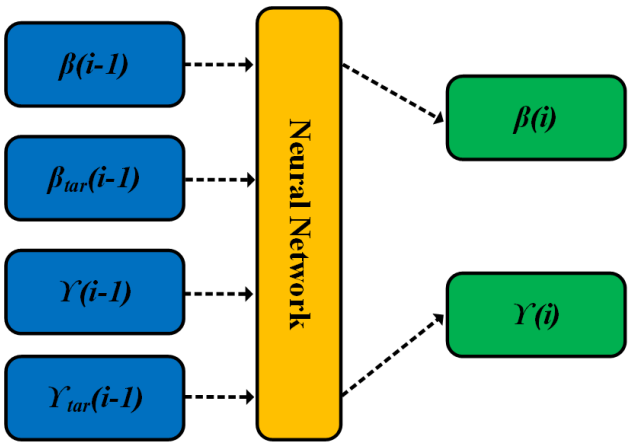


FIGURE 6. Architecture of proposed neural network strategy.

The network takes on the previous yaw rate, the previous target yaw rate, the previous sideslip angle, and the previous target sideslip angle to predict the actual yaw rate and sideslip angle at the current time step.

The model was trained using MATLAB's Deep Learning (DL) Package. A dataset was created using simulated driving

maneuvers. The model was trained using the Levenberg-Marquardt algorithm. The dataset used to train the network is unique to the driving maneuvers used in a double-lane change, and they consist of various magnitudes and approach angles. Five million data points were used in the training set. This same approach can be applied to any combination of steering actions. The innards of the network consist of two layers with three and two nodes, respectively. Hyper-parameter tuning was utilized to acquire high accuracy, as well as minimal computational burden. The tansig and purelin activation functions were used to prevent linearization between the outputs of layers.

$$r_3 = \sum_{i=1}^{10} \left(\beta_{FNN,i} - \beta_{est,i}\right)^2 + \left(\gamma_{FNN,i} - \gamma_{est,i}\right)^2 \quad (15)$$

(15) describes the residual equation for this detection scheme. This metric compares the predicted yaw rate and sideslip angle at the current time step to the FNN's prediction for the actual yaw rate and sideslip angle at the current time step. Its residual graph can be seen in Fig. 7. For the remainder of this paper, this detection strategy will be denoted as DM:3.

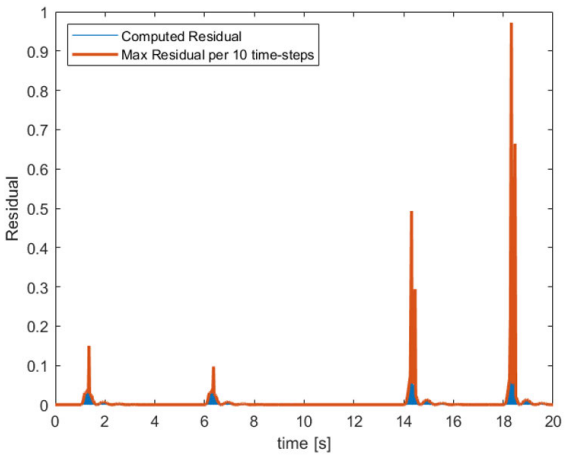


FIGURE 7. Residual metric for proposed DM:3.

D. PERFORMANCE EVALUATION OF DETECTION STRATEGIES

This section describes the performance of each detection method during various cyber-attacks while the vehicle is completing a double-lane change maneuver. First, figures are displayed to illustrate the system's path tracking, yaw-rate tracking, and sideslip angle tracking performance under conditions where no cyber-attack has been launched. This is followed by results and a discussion of the system facing cyber-attacks and how well each detection method performs for each attack scenario.

E. NORMAL OPERATING CONDITIONS WITHOUT CYBER-ATTACK

Fig. 8 depicts the lateral position of the vehicle in normal operating conditions. Fig. 9 depicts the yaw rate of the vehicle in normal operating conditions. Fig 10. depicts the sideslip angle of the vehicle in normal operating conditions. As seen from the figures under normal operating conditions, it is obvious that the control law used for lateral stability control is working. The MPC provides appropriate target yaw rate and sideslip angle values, and the LSCS tracks the desired trajectory commands.

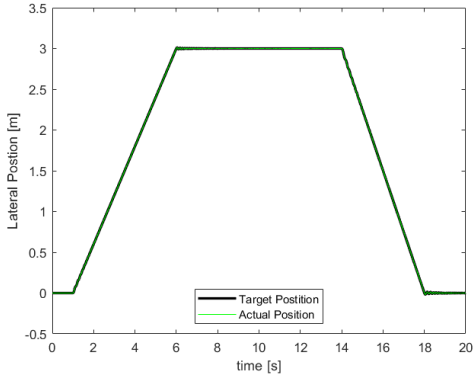


FIGURE 8. Lateral position tracking during double-lane change under no cyber-threat.

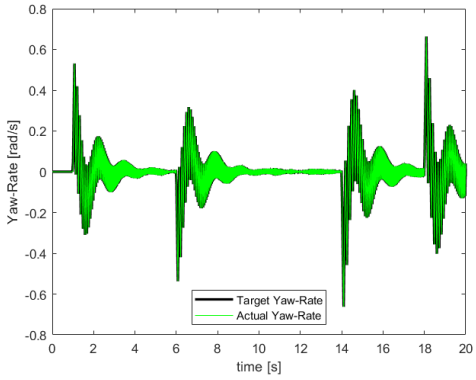


FIGURE 9. Yaw-rate tracking during double-lane change under no cyber-threat.

F. DATA INTEGRITY ATTACK STATISTICS FOR THE THREE DETECTION METHODS

DIAs aim to skew the real value of a signal. This is accomplished by scaling the signal by a value other than one or summing the signal with a value other than zero. (16a) and (16b) describe the scaling scenario for yaw rate and sideslip angle, respectively, and (16c) and (16d) depict the summation attack case.

$$\gamma = m\gamma \quad (16a)$$
$$\beta = m\beta \quad (16b)$$
$$\gamma = \gamma + m \quad (16c)$$
$$\beta = \beta + m \quad (16d)$$

As seen from the graphs, DM:1 and DM:3 manifested the most cyber-threat detections of the three methods. Each method gleaned more satisfactory results as values of m

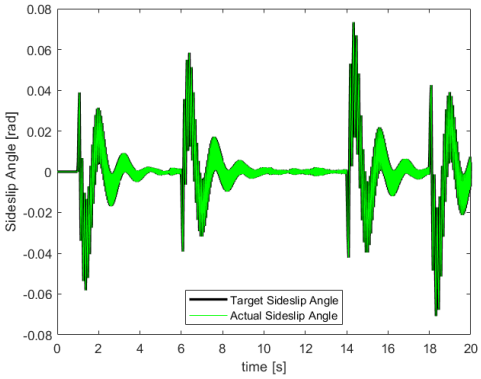


FIGURE 10. Sideslip angle tracking during double-lane change under no cyber-threat.

strayed from one, but DM:2 still paled in performance to its counterparts.

Fig. 11a illustrates the detection response of each of the three detection methods for six different DIAs of this form. In this figure, the empty circles indicate a missed detection for the respective detection method.

The detection proficiency of the three methods for the summation form given by (16c) and (16d) for DIA is depicted in Fig. 11b. Similarly to what is seen in Fig. 11a, the detection methods have the most success for more impactful values of m. DM:2 improves upon its performance seen in the first attack scheme and detects similarly to DM:3.

G. REPLAY ATTACK STATISTICS FOR THE THREE DETECTION METHODS

As stated previously, replay attacks prevent the update of sensor values at each time step, meaning that the same measured signal value will be used at each time step while the replay attack is occurring. Fig. 11c illustrates the detection method's performance in the event of a replay attack. These attacks begin at t=3.2s, and lasts m amount of time.

The effects of a replay attack increase with the length of time that the attack occurs. DM:1 proved to be the least effective detection method for detecting replay attacks. DM:3 produced reliable results for attacks targeting both the yaw rate and sideslip angle.

H. DENIAL OF SERVICE (DOS) ATTACK STATISTICS FOR THE THREE DETECTION METHODS

Detection results in the event of a DOS attack are seen in Fig. 11d. DOS attacks attempt to incapacitate a monitored system by flooding the system with requests for data. In this simulation, DOS attacks are created by sampling the signal under attack at a different rate than the rest of the system. This is simulated by leaving the tampered signal at the normal sample rate of the program and only allowing other signals to update at a decreased rate. This effectively makes the signal updating at normal speed appear to be updating more quickly, thus simulating a DOS attack. For these attack scenarios, the DOS attack lasts the length of the simulation. At the beginning of the maneuver, there is no lateral adjustment command, so it is understandable why no alarm is triggered prior to the double lane change. When the yaw rate is sampled faster than the system's other signals, DM:1 fails to detect the attack, and DM:3 detects the attack much sooner than DM:2. Each detection method sees the DOS attack when the sideslip angle is sampled at a higher rate, but DM:3 is the first to realize the vehicle is under threat.

I. SPECIAL CONSIDERATION FOR LONGITUDINAL SPEED

For the previous cyber-threat examples used in this study, the longitudinal speed was held constant. Therefore, the value seen on the longitudinal speed sensor was seen as a constant value. Since the double-lane change maneuver utilizes a constant speed, attacks of the denial-of-service and replay form will not have any effect. However, both types of data-integrity attacks will malevolently impact the signal.

As seen from Fig. 12, both forms of data-integrity attacks have been placed on the vehicle's speed sensor. For each of these attacks, the attack duration lasted between $t = 3 - 5s$ and the vehicle was still successful in completing the maneuver. Note that DM:2 is not placed on these graphs since it failed to make a threat detection. Both DM:1 and DM:3 were successful in making the detection and performed similarly in their detection times.

V. NUMERICAL COMPARISON OF DETECTION METHOD'S PERFORMANCE

To determine which detection strategy provided the most reliable detection abilities, a scoring metric has been developed that accounts for the method's ability to detect a cyber-attack and the time lapse between attack initiation and detection time.

In this study, there are effectively eight different types of attacks. Each attack has various subsets of attacks. As an example, the scaling DIA uses six values for m. A vector is made for each detection method, and the elements of the vector depict its performance for each of the eight types of attacks. Each element of the respective vectors depicts the method's performance for each of the attack schemes.

$$\mathrm{DM}(i,1) = \sum_{n=1}^{\#ofAttaks} (t_{i,\mathrm{start}} - t_{i,n_{det}}) \tag{17}$$

In (17), DM$(i, 1)$ stands for the i^{th} element of a detection method's score vector. Also, $t_{i,\mathrm{start}}$ is the start time for the i^{th} type of attack, and $t_{i,n_{\mathrm{det}}}$ is the time at which the detection strategy noticed the presence of the n^{th} attack of the i^{th} type of attack. If the detection method fails to detect the attack, the end of simulation time is used, which is $t = 20$s.

The elements of the detection method's score vectors are then normalized by (18). The vectors are normalized to nullify the effects of comparing different types of attacks.

$$\mathrm{DM} = \frac{\mathrm{DM} - \mathrm{DM}_{min}}{\mathrm{DM}_{max} - \mathrm{DM}_{min}} \tag{18}$$

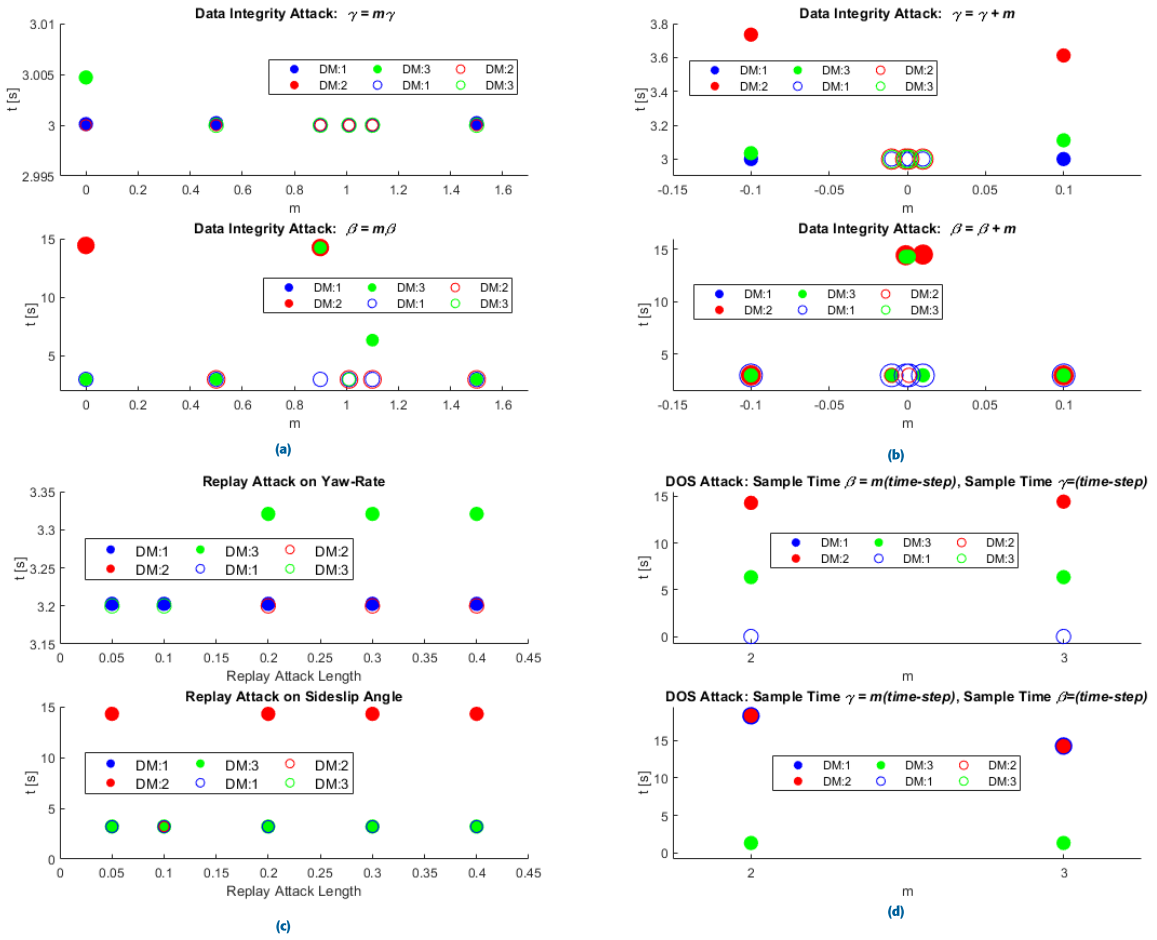


FIGURE 11. NOTE (Filled in circle indicates successful detection whereas hollow circle indicates missed detection) Detection method's detection time statistics for (a) Data integrity in the form of a scalar, (b) Data integrity attack in summation form of the true values, (c) Replay attack, and (d) DOS attack.

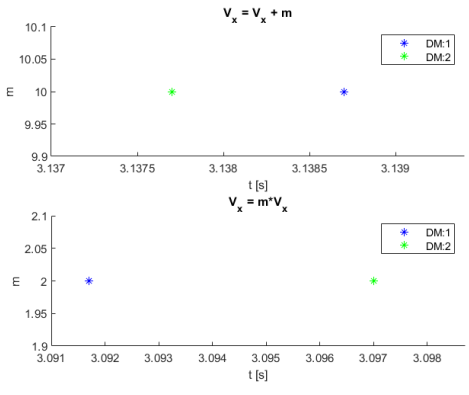


FIGURE 12. Detection method performance for attack on cruising speed.

Once the normalized scoring vectors have been created, their elements are then summed to compute a final score. A smaller score indicates more successful attack detections and smaller time windows between attack initiation and attack detection. Table 2 provides the detection method's scores given the scoring scheme created through (17) and (18). As seen from the table, DM:3 outperformed DM:1 and DM:2, indicating that it provided the most security to the vehicle's LSCS.

TABLE 2. Detection method's scores using (17)-(18).

Detection Method	Score
DM: 1 [11]	4.8482
DM: 2 [11]	6.6022
DM: 3 [FNN]	2.9199

As seen from the table, DM:3 outperformed DM:1 and DM:2, indicating that it provided the most security to the vehicle's LSCS.

VI. CONCLUSION AND FUTURE WORK

This study utilized MATLAB/Simulink to model an electric vehicle, its lateral stability control system, and its electric motoring system. Three different detection criteria were developed that compare the system's target, estimated, and predicted lateral trajectories. Under the test conducted, it is

apparent that each of the detection methods proved to be effective at detecting cyber threats. To improve upon this study, more variants of cyber threats should be investigated. Also, a threshold on the residual bands should be developed that gives room for the dynamic behavior of the system. Overall, however, the residual detection strategy proved to be an effective metric for detecting cyber-security threats in the system.

ACKNOWLEDGMENT

The authors would like to thank the Warren H. Owen Distinguished Professorship Endowment for its support of the research effort and also would like to thank the support and resources provided by the Secure Energy and Automation Laboratory (SEAL) and Real Time COntrols and Optimization Laboratory (RT-COOL) laboratories in facilitating this research.

REFERENCES

[1] L. Timilsina, P. H. Hoang, A. Moghassemi, E. Buraimoh, P. K. Chamarthi, G. Ozkan, B. Papari, and C. S. Edrington, "A real-time prognostic-based control framework for hybrid electric vehicles," *IEEE Access*, vol. 11, pp. 127589–127607, 2023.

[2] L. Timilsina, P. H. Hoang, A. Arsalan, B. R. Badr, G. Ozkan, B. Papari, and C. S. Edrington, "Degradation abatement in hybrid electric vehicles using data-driven technique," *Transp. Res. Proc.*, vol. 70, pp. 52–60, Jan. 2023.

[3] A. Arsalan, L. Timilsina, B. Papari, G. Muriithi, G. Ozkan, P. Kumar, and C. S. Edrington, "Cyber attack detection and classification for integrated on-board electric vehicle chargers subject to stochastic charging coordination," *Transp. Res. Proc.*, vol. 70, pp. 44–51, Jan. 2023.

[4] L. Timilsina, A. Moghassemi, E. Buraimoh, A. Arsalan, P. K. Chamarthi, G. Ozkan, B. Papari, and C. Edrington, "Impact of vehicle-to-grid (V2G) on battery degradation in a plug-in hybrid electric vehicle," in *Proc. SAE Tech. Paper Ser.*, Apr. 2024, doi: 10.4271/2024-01-2000.

[5] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental security analysis of a modern automobile," in *Proc. IEEE Symp. Secur. Privacy*, May 2010, pp. 447–462.

[6] A. Al Mamun, M. A. Al Mamun, and A. Shikfa, "Challenges and mitigation of cyber threat in automated vehicle: An integrated approach," in *Proc. Int. Conf. Electr. Electron. Technol. Automot.*, Jul. 2018, pp. 1–6.

[7] X. Shao, C. Dong, and L. Dong, "Research on detection and evaluation technology of cybersecurity in intelligent and connected vehicle," in *Proc. Int. Conf. Artif. Intell. Adv. Manuf. (AIAM)*, Oct. 2019, pp. 413–416.

[8] P. Darby and R. Gottumukkala, "Decentralized computing techniques in support of cyber-physical security for electric and autonomous vehicles," in *Proc. IEEE Green Technol. Conf. (GreenTech)*, Apr. 2019, pp. 1–5.

[9] S. Gifei Cas. Aionoaie and A. Salceanu, "Autonomous and electrical vehicles development using optimized processes defined by cyber security and safety management system," in *Proc. Int. Conf. Electromechanical Energy Syst. (SIELMEN)*, Oct. 2021, pp. 257–261.

[10] A. Arsalan, B. Papari, S. I. Rahman, L. Timilsina, A. Moghassemi, G. Muriithi, G. Ozkan, C. Edrington, and E. Buraimoh, "Machine learning approach for open circuit fault detection and localization in EV motor drive systems," SAE Tech. Paper. 2024-01-2790, 2024.

[11] L. Guo and J. Ye, "Cyber-physical security of electric vehicles with four motor drives," *IEEE Trans. Power Electron.*, vol. 36, no. 4, pp. 4463–4477, Apr. 2021.

[12] L. Guo, B. Yang, and J. Ye, "Enhanced cyber-physical security of steering stability control system for four-wheel independent drive electric vehicles," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2020, pp. 1240–1245.

[13] B. L. Boada, M. J. L. Boada, and V. Diaz, "Vehicle sideslip angle measurement based on sensor data fusion using an integrated ANFIS and an unscented Kalman filter algorithm," *Mech. Syst. Signal Process.*, vols. 72–73, pp. 832–845, May 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0888327015004999

[14] B. Huang, S. Wu, S. Huang, and X. Fu, "Lateral stability control of four-wheel independent drive electric vehicles based on model predictive control," *Math. Problems Eng.*, vol. 2018, pp. 1–15, Jan. 2018.

[15] H. Zhou, F. Jia, H. Jing, Z. Liu, and L. Güvenç, "Coordinated longitudinal and lateral motion control for four wheel independent motor-drive electric vehicle," *IEEE Trans. Veh. Technol.*, vol. 67, no. 5, pp. 3782–3790, May 2018.

[16] K. Yang, D. Dong, C. Ma, Z. Tian, Y. Chang, and G. Wang, "Stability control for electric vehicles with four in-wheel-motors based on sideslip angle," *World Electric Vehicle J.*, vol. 12, no. 1, p. 42, Mar. 2021.

[17] Z. Yong-qiang, C. Quan-shi, and Z. Ping-xia, "The research of stability performance of five-axle all wheel driving vehicles with electric wheels basing on direct yaw control and traction control system," in *Proc. 2nd Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2012, pp. 1451–1454.

[18] J.-S. Hu, Y. Wang, H. Fujimoto, and Y. Hori, "Robust yaw stability control for in-wheel motor electric vehicles," *IEEE/ASME Trans. Mechatronics*, vol. 22, no. 3, pp. 1360–1370, Jun. 2017.

[19] J. Zhang and H. Zhang, "Vehicle lateral stability control based on single neuron network," in *Proc. Chin. Control Decis. Conf.*, May 2010, pp. 290–293.

[20] P. C. Krause, O. Wasynczuk, S. D. Sudhoff, and S. Pekarek, *Analysis of Electric Machinery and Drive Systems*, vol. 2. Hoboken, NJ, USA: Wiley, 2002.

[21] S. B. Ozturk and H. A. Toliyat, "Direct torque control of brushless DC motor with non-sinusoidal back-EMF," in *Proc. IEEE Int. Electric Mach. Drives Conf.*, May 2007, pp. 165–171.

[22] S. Rambabu, "Modeling and control of a brushless DC motor," M.S. thesis, Power Control Drives Technol., Dept. Elect. Eng., Nat. Inst. Technol., Rourkela, Odisha, 2007.

[23] J. Nan, H. Li, W. Cao, Y. Wang, and W. Zhao, "Research on improvement and experiment for cyber security of automotive electronic and electrical architecture," in *Proc. IEEE 7th Int. Conf. Intell. Transp. Eng. (ICITE)*, Nov. 2022, pp. 400–405.

[24] L. Guo, J. Ye, and B. Yang, "Cyberattack detection for electric vehicles using physics-guided machine learning," *IEEE Trans. Transport. Electrific.*, vol. 7, no. 3, pp. 2010–2022, Sep. 2021.

[25] L. Guo, B. Yang, J. Ye, H. Chen, F. Li, W. Song, L. Du, and L. Guan, "Systematic assessment of cyber-physical security of energy management system for connected and automated electric vehicles," *IEEE Trans. Ind. Informat.*, vol. 17, no. 5, pp. 3335–3347, May 2021.

[26] B. Yang, L. Guo, F. Li, J. Ye, and W. Song, "Impact analysis of data integrity attacks on power electronics and electric drives," in *Proc. IEEE Transp. Electrific. Conf. Expo. (ITEC)*, Jun. 2019, pp. 1–6.

[27] L. Guo, J. Ye, and L. Du, "Cyber–physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyber-attacks," *IEEE Trans. Transport. Electrific.*, vol. 7, no. 2, pp. 636–648, Jun. 2021.

[28] R. Gottumukkala, R. Merchant, A. Tauzin, K. Leon, A. Roche, and P. Darby, "Cyber-physical system security of vehicle charging stations," in *Proc. IEEE Green Technol. Conf.(GreenTech)*, Apr. 2019, pp. 1–5.

[29] E. Gumrukcu, A. Arsalan, G. Muriithi, C. Joglekar, A. Aboulebdeh, M. A. Zehir, B. Papari, and A. Monti, "Impact of cyber-attacks on EV charging coordination: The case of single point of failure," in *Proc. 4th Global Power, Energy Commun. Conf. (GPECOM)*, Jun. 2022, pp. 506–511.

[30] S. Acharya, Y. Dvorkin, H. Pandžic, and R. Karri, "Cybersecurity of smart electric vehicle charging: A power grid perspective," *IEEE Access*, vol. 8, pp. 214434–214453, 2020.

[31] P. R. Badr, B. Papari, A. Robison, C. S. Edrington, A. Abulebdah, M. A. Zehir, and E. Hammad, "Holistic performance benchmarking in power systems with distributed control under disruptive cyberattacks," in *Proc. IEEE Transp. Electrific. Conf. Expo (ITEC)*, Jun. 2022, pp. 640–646.

[32] M. Girdhar, J. Hong, Y. Yoo, and T.-J. Song, "Machine learning-enabled cyber attack prediction and mitigation for EV charging stations," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Jul. 2022, pp. 1–5.

[33] J. Kandasamy, S. Arunagirinathan, P. Sivaraj, M. Pameela, G. T. Subham, and R. Nagarajan, "Detection of cyber attack in electric vehicles using ALSTM based machine learning," in *Proc. 4th Int. Conf. Inventive Res. Comput. Appl. (ICIRCA)*, Sep. 2022, pp. 596–600.

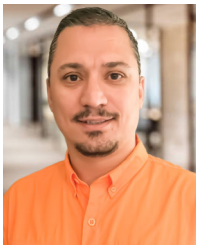
DOUGLAS G. SCRUGGS received the bachelor's and master's degrees in electrical engineering from Clemson University. He is currently a Turbo Generator Engineer with Siemens Energy. He has completed three CO-OP rotations with the JTEKT Koyo's Machine Design Group. He has also completed three summer internships with Savannah River Site.

LAXMAN TIMILSINA (Member, IEEE) received the B.E. degree in electrical engineering from the Institute of Engineering, Tribhuvan University, Nepal, in 2016, the M.Sc. degree in distributed generation in electrical engineering from the Institute of Engineering, in 2019, and the Ph.D. degree in electrical engineering from Clemson University, in May 2024, under the mentorship of Dr. Christopher S. Edrington. Transitioning to the next phase of his academic journey, he enrolled with Clemson University, in Fall 2021, to pursue the Ph.D. degree. Concurrently, he was a Graduate Research Assistant with the Real-Time COntrol and Optimization Laboratory (RT-COOL), The Holcombe Department of Electrical and Computer Engineering (ECE), Clemson University, where he is currently a Postdoctoral Researcher Fellow with RTCOOL. His research interests include electrified vehicles, integration of renewable energy, ship power systems, and smartgrids.

BEHNAZ PAPARI (Senior Member, IEEE) received the B.S. degree in electrical engineering from the University of Bushehr, in 2008, the M.Sc. degree in electrical engineering from the K. N. Toosi University of Technology, Iran, in 2011, and the Ph.D. degree in electrical and computer engineering from Florida State University, USA, in 2018. Prior to joining the Department of Automotive Engineering and Electrical and Computer Engineering, Clemson University, in Spring 2022, she was an Assistant Professor with the Department of Marine Engineering Technology, Texas A&M University, and an Assistant Professor of Practice with the Energy Production and Infrastructure Center (EPIC) for three years with UNC Charlotte, where she taught at undergraduate and graduate levels. Her background is in power systems controls, with an emphasis on modeling, analysis, planning, and AI-based optimization. Her current research interests include distributed controls and secure control frameworks under uncertainty, applications on energy system modeling, stochastic optimization, and electric vehicle, including electric and hybrid-electric and ESSs.

ALI ARSALAN (Graduate Student Member, IEEE) received the bachelor's degree in electronics engineering from UCET, IUB, Pakistan, in 2015, and the master's degree in electrical engineering from UET, Lahore, Pakistan, in 2019. He is currently pursuing the Ph.D. degree in automotive engineering with Clemson University, SC, USA. After that, he was a Laboratory Engineer with the Khwaja Fareed University of Engineering and Information Technology (KFUEIT), Pakistan, from January 2017 to August 2022. He is also a Graduate Research Assistant with the Secure Energy and Automation Laboratory (SEAL), International Center for Automotive Research (ICAR), Greenville. His research interests include optimization, microgrids, energy management, EV technologies, cyber security, and power system resiliency toward cyber threats.

GRACE MURIITHI (Graduate Student Member, IEEE) received the B.Sc. degree in electrical engineering from the Jomo Kenyatta University of Agriculture and Technology, Kenya, and the M.Sc. degree in electrical engineering from the University of Cape Town, South Africa. She is currently pursuing the Ph.D. degree in automotive engineering with the International Centre for Automotive Research, Clemson University. She is currently undertaking research in resilience and security enhancement of cyber-physical systems, with a particular focus on (hybrid) electric vehicles (HEVs) and electric vehicle charging stations (EVCSs). Her research interests include cyber-physical systems security, machine learning, energy management, microgrids, and vulnerability analysis in advanced control systems.



GOKHAN OZKAN (Senior Member, IEEE) received the B.Sc. degree from the Electrical Education Department, Marmara University, in 2006, the B.Sc. (as a Valedictorian) and M.Sc. degrees from the Energy System Engineering Department, Erciyes University, in 2014 and 2016, respectively, and the Ph.D. degree from the Electrical and Computer Engineering Department, Florida State University, in 2019. He joined Clemson University as a Postdoctoral Fellow, in 2020. He has been a Research Assistant Professor with The Holcombe Department of Electrical and Computer Engineering, since 2021. He is currently the Research Lead with the Energy Innovation Center, North Charleston, and also the Manager of the Real-Time COntrol and Optimization Laboratory (RT-COOL). His main research interests include power systems and DER integration, model predictive control in power converters and drives, active thermal management and fault-tolerant control, distributed controls, power and EM, real-time power distribution system modeling, simulation, co-simulations, and hardware-in-the-loop instantiation.

CHRISTOPHER S. EDRINGTON (Senior Member, IEEE) received the B.S. degree in engineering from Arkansas State University, in 1999, and the M.S. and Ph.D. degrees in electrical engineering from Missouri University of Science and Technology, in 2001 and 2004, respectively. He was both a GAANN and IGERT Fellow of Missouri University of Science and Technology. From 2004 to 2007, he was an Assistant Professor in electrical engineering with the College of Engineering, Arkansas State University. From 2007 to 2019, he held the ranks of an Assistant Professor, an Associate Professor, and a Full Professor in electrical and computer engineering with the FAMU-FSU College of Engineering and was the Lead of the Energy Conversion and Integration Thrust, Florida State University-Center for Advanced Power Systems. In 2019, he joined Clemson University as the Warren H. Owen Distinguished Professor of Electrical and Computer Engineering, where he leads the Real-Time COntrol and Optimization Laboratory (RT-COOL). Additionally, he is the Associate Director of Industry Relations with the VIPR-GS Center, Clemson University. His research interests include modeling, simulation, optimization, and control of: electromechanical drive systems, applied power electronics, integration of renewable energy, storage, pulse power loads, and hardware in the loop (HIL) VV&A experimentation.