12-2023

Cyber-Threat Detection Strategies Governed by an Observer and a Neural-Network for an Autonomous Electric Vehicle

Douglas Scruggs
dgscrug@g.clemson.edu

Recommended Citation

Scruggs, Douglas, "Cyber-Threat Detection Strategies Governed by an Observer and a Neural-Network for an Autonomous Electric Vehicle" (2023). *All Theses*. 4186.
https://tigerprints.clemson.edu/all_theses/4186

Cyber-Threat Detection Strategies Governed by an Observer and a Neural-Network for an Autonomous Electric Vehicle

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Masters of Science
Electrical Engineering

by
Douglas Gettys Scruggs
December 2023

Accepted by:
Dr. Behnaz Papari, Committee Chair
Dr. Christopher Edrington
Dr. Fatemeh Afghah

Abstract

A pathway to prevalence for autonomous electrified transportation is reliant upon accurate and reliable information in the vehicle's sensor data. This thesis provides insight as to the effective cyber-attack placements on an autonomous electric vehicle's lateral stability control system (LSCS). Here, Data Integrity Attacks, Replay Attacks, and Denial-of-Service attacks are placed on the sensor data describing the vehicle's actual yaw-rate and sideslip angle. In this study, there are three different forms of detection methods. These detection methods utilize a residual metric that incorporate sensor data, a state-space observer, and a Neural-Network. The vehicle at hand is a four-motor drive autonomous electric vehicle that is propelled using 4-pole, 3-phase Brushless DC motors. Each motor is controlled using the Direct-Torque control motor control scheme that provides fast output torque response time. This vehicle is controlled via multiple layers of control. A Model Predictive Control Layer is used to discern what lateral trajectory commands minimize the difference between the requested and actual lateral position of the vehicle. These lateral motions are discovered through a Linear-Quadratic Regulator. This study was develop using the MATLAB Simulink environment.

Dedication

I am dedicating this thesis to both my mother and father. Both of my parents have always provided me with resilient support and calculated guidance. I am truly blessed to have such kind-hearted and devoted parents. Without them, no part of this entire process would have been possible.

Acknowledgments

I would like to acknowledge the S.E.A.L (Secure Energy and Automation Laboratory) and the RT-COol (Real-Time Control and Optimization Laboratory) lab groups. Every individual in these groups has made a both distinguished and positive impact on my graduate career. I would also like to express a unique and sincere gratitude to Dr. Papari for both her patience and sound guidance through this academic process. Repeatedly and unwaveringly, she has steered me towards conducting graduate level research that I would not have been able to complete on my own. In addition, I would like to express earnest thanks for Dr. Kumar's effort and support while completing my thesis. Dr. Kumar has been a both key and fundamental player in this research.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Cyber-Security in Electric Vehicles

An increase in intelligence seen by our population's modes of transportation is paralleled by an increase in the potential avenues for cyber-attacks. As stated in [1], there are expected to be as many as 125 million electric vehicles on the streets by 2030. The prevalence of electric vehicles brings reasonable concern to both the cyber physical security of a vehicle on the road, as well as for the vehicle's ability to make a secure charge. Cyber-Security challenges regarding electric vehicle infrastructure are discussed in [2]. In [2], it is discussed that insecure charging stations do not only provide an opportunity to cause harm for the direct user, but insecure charging points can also induce problems on the stability of the whole power grid due to the interconnections of the entire system. The authors of [3] explore the vulnerabilities in charging infrastructure. A major concern for an end user in this study involves the payment process for charging one's electric vehicle with a public charger. The cyber-physical security of electric vehicle charging stations is presented in [4]. Cyber-Attacks of concern include Man-in the-Middle Attacks, Denial-of-Service Attacks, SQL Injection Attacks, and Malware Attacks. This list is expanded on in [5], were additional vulnerabilities include, Server-side request forgery, Cross-site scripting, Comma-Separated value injection, Cross-site request forgery, and External Media injection. An example method for increasing the cyber-security in charging stations is given in [6]. The authors promote a human-less multi-factor authentication protocol to charge their vehicles, to prevent hackers from ceasing confidential information on their charging cards. A strategy to hamper Message Tampering Attacks on charging stations is given in [7]. This method explores a cohesive protocol between user authentication and a central server. Susceptible points of cyber-attack interfaces are described in [8] and include charging ports, power electronics, controllers, and local generation.

As expected, cyber-attacks on vehicle control units have increased with the intelligence of vehicle infrastructure. Cyber-Physical attacks on an electric vehicle have the potential to inflict physical consequences on the vehicle itself. Recently, a Tesla Model X was hacked as seen in [9]. In this instance, firmware was rewritten over the Bluetooth key fob. Another cyber breach is seen in [10], where a Jeep Grand Cherokee was remotely hijacked while moving. This does not only present lethal danger for the driver, but also those sharing the rode with the driver. Tesla takes precautionary measures against cyber-threats by pushing out updates once a threat has been identified as seen in [11]. Research interest as to to Cyber-Physical security have seen in an increase in research recently. In [12], the authors investigate the Cyber-Physical security in a vehicle's power train. The author's of this paper convey that hackers can leverage the same attack strategies used on electric vehicle chargers to attack a vehicle, given the hackers have prior knowledge of the system. In [13], sophisticated cyber-attacks are placed on a hybrid electric vehicle. To detect the presence of an attack, a probability metric is created that alludes to the probability of there being an attack. The authors of [14] conduct a study where the effects of a cyber-attack placed on a vehicle's electrical control unit are analyzed. In addition to electric vehicles, the cyber-security of autonomous vehicles is evaluated in [15]. To build upon previously described methods, artificial intelligence for the sake of physical cyber-security is studied in [16]. Here, an LSTM architecture is utilized to detect cyber-threats. Inputs to the network include yaw-rate and sideslip angle from previous time-steps.

1.2 Lateral Stability Control

In the field of automotive and controls, there a multitude of methods for controlling the lateral stability of a vehicle. The vehicle's lateral stability is commonly controlled through the vehicle's yaw-rate and sideslip angle. A vehicle's yaw-rate can be defined as the speed at which the vehicle rotates around its vertical axis. A vehicle's yaw-rate is often measured by the means of a yaw-rate sensor, that records the yaw-rate in radians per second. As discussed in [17], a common application of yaw-rate sensors in commercial vehicles, is to compare the vehicle's actual yaw-rate to a reference value, and then apply necessary steering actions or braking forces for the vehicle to meet its reference. Sideslip anlge, or slip angle, is another lateral metric of a moving vehicle that is described as the angle between the vehicle's orientation and the direction of the vehicle's movement. In [18], the sideslip angle is visually described as the angle between the vehicle's forward longitudinal direction and the vehicle's velocity vector. In practice, sideslip angle is commonly estimated via an observer or gleaned from measurements made by other vehicular sensors. In [19], it is discussed that sideslip angle sensors are not practical in application due to their expense. Instead, the authors propose an observer based strategy utilizing a Kalman Filter to make an estimate as to the sideslip angle. A comprehensive study of the methods to make a sideslip angle estimation have been provided in [20]. One of the discussed methods includes a machine learning approach utilizing a Neural-Network. Here, sensor values from previous time-steps describing wheel speed, longitudinal and lateral acceleration, yaw-rate, roll-rate, and steering wheel angle are used as inputs to the Neural-Network. This information provided the model sufficient information to make a sideslip angle prediction at the current time-step.

A vehicle's Lateral Stability Control System, LSCS, is responsible for maintaining a vehicle's lateral stability by preventing the vehicle from entering states where the driver of the vehicle loses control. A common tool for controlling a vehicle's LSCS is Model Predictive Control. In [21], a MPC objective function is developed that brings the vehicle's sideslip angle to a stable region if the vehicle's sideslip angle causes instability. Here, the MPC discovers what lateral maneuvers would optimize their objective function. The authors of [22] also utilize MPC to obtain lateral stability. The goal of this MPC strategy is to bring the vehicle to the target yaw-rate, lateral speed, and wheel slip ratio. The control inputs used in this study to minimize their objective function are additional torque moments. A Non-Linear Model Predictive Control, NMPC, is adopted in [23] to adopt lateral stability. For this controller design, the yaw-rate and sideslip angle are brought to reference values by the NMPC. The NMPC control inputs are the angle of the front wheels as well as the braking force of the tires. In [24], the authors develop three distinct regions in a 2D plane which describe the vehicle's current yaw-rate and sideslip angle. These three regions describe whether the vehicle is stable, critically stable, or unstable. The author's MPC strategy aims to either move the vehicle towards or keep the vehicle in its stable region.

In addition to MPC, machine learning techniques have also been utilized to maintain lateral stability. Unlike physics based approaches like MPC, machine learning techniques utilize an abundance of data. Data describing the system the machine learning model will be placed in is used to train models like a Neural-Network to predict outputs of a given system. A common problem with this approach involves the absence of a robust data set describing the system. A common approach to solve this problem is to create the data set by means of simulation. In [25], the authors propose a single neuron Neural-Network to track a reference yaw-rate and sideslip angle. For this model, the difference between target yaw-rate and and actual yaw-rate, as well as the difference between target sideslip angle and actual sideslip angle are used as inputs. The output of the network is an additional yaw-moment for the vehicle to track target values. Another instance of lateral stability controlled through machine learning is seen in [26]. In [26], the authors study a vehicle with fourteen degrees of freedom. For this network, the vehicle's target yaw-rate and actual yaw-rate are used as inputs. The output of the network is the additional yaw-moment necessary to track the reference yaw-rate.

1.3 Motoring Schemes in Electric Vehicles

Propulsion power in an electric vehicle is created by the output of its electric motoring system. Common types of electric motors used in EVs include Brushed DC motors, Brushless DC motors, Induction machines, Permanent Magnet Synchronous machines, and Switch Reluctance machines. Different types of motors offer different types of benefits and drawbacks. The authors of [27] provide a survey on the strengths and weaknesses of different types of electric motors for vehicular applications. In this study, it is shown that Brushless DC Machines are very efficient. This is due to the fact that they do not have coils on their rotor, and therefore do not sustain the same losses as machines with coils on their rotor. This survey study concludes by saying the prevalence of Induction machines and Brushless DC machines in electric vehicles is a consequence of their efficiency, high power density, and their cost. The study conducted in [28] also makes comparisons between different types of machines in electric vehicles. While Induction machines have seen a surge in popularity in electric vehicles, their study notes that Induction machines have a small power factor as well as larger losses at high speeds. The study also states that car manufactures such as Honda, Toyota, and Nissan utilize Permanent Magnet Synchronous machines. While these machines have the same efficiency benefits as machines without coils on the rotor, they do suffer from a a smaller range of speeds that deliver constant power.

Arguments for Brushless DC motors in electric vehicles are made in [29] when placed in electric vehicles. Reasonable support for the motor is gained through its lack of maintenance, the motor's volume, and again, its efficiency. These points are reemphasized in [30]. The authors of [30] mention that one of the bigger flaws associated with Brushless DC motors is torque ripple. They suggest that a stronger rotor core can reduce this effect. A comprehensive study is conducted in [31] for Brushless DC machines in electric vehicles. The paper provides an outline for sizing these machines for a vehicle and also provides data describing the machine's prowess.

When designing an electric vehicle, not only is the type of motor one of the design considerations, but also the method used to control the motor. Principle operation of the motoring portion of an electric vehicle is reliant upon both a DC Link Voltage and a converter. DC Link Voltage acts as a power supply for the converter. The converter is the power source for the motor and can be seen as either a voltage source or current source to the motor. The type of source the motor sees the converter as, is dependent upon the type of control scheme that is used. All motor control schemes control the motor by determining when to close or open the switches in the converter. A survey on motor control strategies in electric vehicles is seen in [32]. The purpose of this study is to draw comparisons between Direct Torque Control and Field Oriented Control for electric vehicle applications. The popularity of Direct Torque Control is noted in [33], [34], and [35]. Popularity stems from the simplicity of the control algorithm as well as the precise torque response.

Chapter 2

Vehicle Model Designing

The objective of this study's vehicle model is for the vehicle to complete a double lane change maneuver. 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 [36].

Fig. 2.1 depicts the system's structure as well as the interactions between the control layers. The devil in Fig. 2.1 depicts the cyber-attack targets.

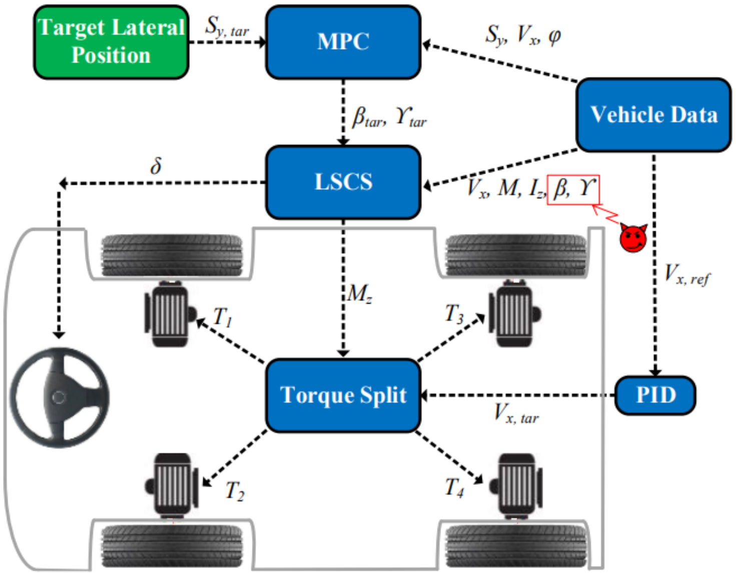

Figure 2.1: Vehicle Control System Diagram

2.1 Lateral Movement Discovered through MPC

If an EV's LSCS is placed under a cyber-attack, 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. Model Predictive Control, (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 Eq. 2.1 where V_x is longitudinal velocity, t_p is the time of the future horizon, and φ is heading angle.

$$\begin{multline} s_y(t+t_p) = (t_p - t) * (V_x * sin(\gamma(t_p) * (t_p - t) + \varphi(t)) + \\ V_x * tan(\beta(t_p)) * cos(\gamma(t_p) * (t_p - t) + \varphi(t))) + s_y(t) \quad (2.1) \end{multline}$$

Once the predicted lateral position has been found, Eq. 2.2 is used to determine what values of β and γ bring the vehicle closest to the target location.

$$min \int_{t}^{t_p} (s_y(t_p) - s_{y,ref}(t))^2 \, dt \quad (2.2)$$

The optimal trajectory commands are then used as reference values for the LSCS.

2.2 Vehicular State-Space System

The purpose of the LSCS is to bring the vehicles 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. In order to create the state-space system, differential equations describing the time derivatives of the systems must be created.

$$\frac{d}{dt}\gamma(t) = \frac{L_f F_{yf}(t) - L_r F_{yr}(t) + M_z(t)}{I_x} \tag{2.3}$$

$$\frac{d}{dt}\beta(t) = \frac{F_{yf}(t) + F_{yr}(t)}{v_x M} - \gamma(t) \tag{2.4}$$

In Eq. 2.3 and Eq. 2.4, 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_x is the vehicle's moment of inertia, and m is the vehicle's mass. F_{yf} and F_{yr} denote the lateral force at the vehicle's front and rear tires.

Lateral force is a function of the sideslip angle of the wheels, α. α can be approximated by utilizing Eq. 2.5 and Eq. 2.6.

$$\alpha_f(t) = \beta(t) + \frac{L_f}{v_x}\gamma(t) - \delta(t) \tag{2.5}$$

$$\alpha_r(t) = \beta(t) + \frac{L_r}{v_x}\gamma(t) \tag{2.6}$$

Since the lateral force is a function of α, a force calculation can be made for the respective position of the wheels given Eq. 2.7.

$$F_y(t) = -2C_y\alpha(t) \tag{2.7}$$

By utilizing the equations describing the time derivative of the states, and the lateral force equations, the control matrix and input matrix can be created. They are seen in Eq. 2.8 and Eq. 2.9 respectively.

$$A = \begin{bmatrix} \frac{-2*(C_{yf}+C_{yr})}{V_x*m} & -1 - \frac{2*(L_f*C_{yf}-L_r*C_{yr})}{V_x^2*m} \\ \frac{-2*(L_f*C_{yf}-L_r*C_{yr})}{I_x} & \frac{-2*(L_f*^2C_{yf}-L_r^2*C_{yr})}{I_x*V_x} \end{bmatrix} \tag{2.8}$$

$$B = \begin{bmatrix} \frac{2*C_{yf}}{V_x*m} & 0 \\ \frac{2*C_{yf}*L_f}{I_x} & \frac{1}{I_x} \end{bmatrix} \tag{2.9}$$

In Eq. 2.8 and Eq. 2.9, C_y represents cornering stiffness which is different for the front and rear axles.

$$\begin{bmatrix} \beta^{'} \\ \gamma^{'} \end{bmatrix} = A \begin{bmatrix} \beta \\ \gamma \end{bmatrix} + B \begin{bmatrix} \delta \\ M_z \end{bmatrix} \tag{2.10}$$

Eq. 3.12 depicts the entire state space equation for the LSCS.

As stated previously, a LQR is used to bring the vehicles 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. The gain matrix is found using Eq. 2.11, where the gain matrix minimizes cost. Gain matrix K is found offline and is applied during simulation.

$$J = \int_0^\infty (x^T Qx + u^T Ru + 2x^T Nu)\, dt \tag{2.11}$$

The inputs sent to the LSCS are then calculated using Eq. 2.12.

$$\begin{bmatrix} \delta \\ M_z \end{bmatrix} = -K \begin{bmatrix} \beta - \beta_{ref} \\ \gamma - \gamma_{ref} \end{bmatrix} \tag{2.12}$$

2.3 Longitudinal Control and Torque Split

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 Eq. 2.13, where r_w is 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.

$$T_{dem} = r_w(Ma_r + \frac{1}{2}\rho_a A_f C_d v_x^2 + Mg[sin(\theta) + fcos(\theta)]) \tag{2.13}$$

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 Eq. 2.13.

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 Eq. 2.14 and Eq. 2.15 respectively.

$$T_{ref,1} = \frac{1}{4}T_{dem} - \Delta T_{ref,1} \tag{2.14}$$

$$T_{ref,3} = \frac{1}{4}T_{dem} - \Delta T_{ref,3} \tag{2.15}$$

The delta component of these equations are given by Eq. 2.16 and Eq. 2.17

$$\Delta T_{ref,1} = \frac{L_f r_w}{(L_f + L_r)L_d} M_z \tag{2.16}$$

$$\Delta T_{ref,3} = \frac{L_r r_w}{(L_f + L_r)L_d} M_z \tag{2.17}$$

The output torque of motor 2 and motor 4 are given by 2.18 and 2.19.

$$T_{ref,2} = \frac{1}{4}T_{dem} - 2\Delta T_{ref,1} \tag{2.18}$$

$$T_{ref,4} = \frac{1}{4}T_{dem} - 2\Delta T_{ref,3} \tag{2.19}$$

Vehicle specifications for this study are given in Table 2.1

2.4 Lateral Tracking Performance

The objective of this chapter's section is to illustrate the ability of this vehicular system model to execute a double-lane change maneuver. The standard procedure for this study involves

Table 2.1: Vehicle Parameters

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

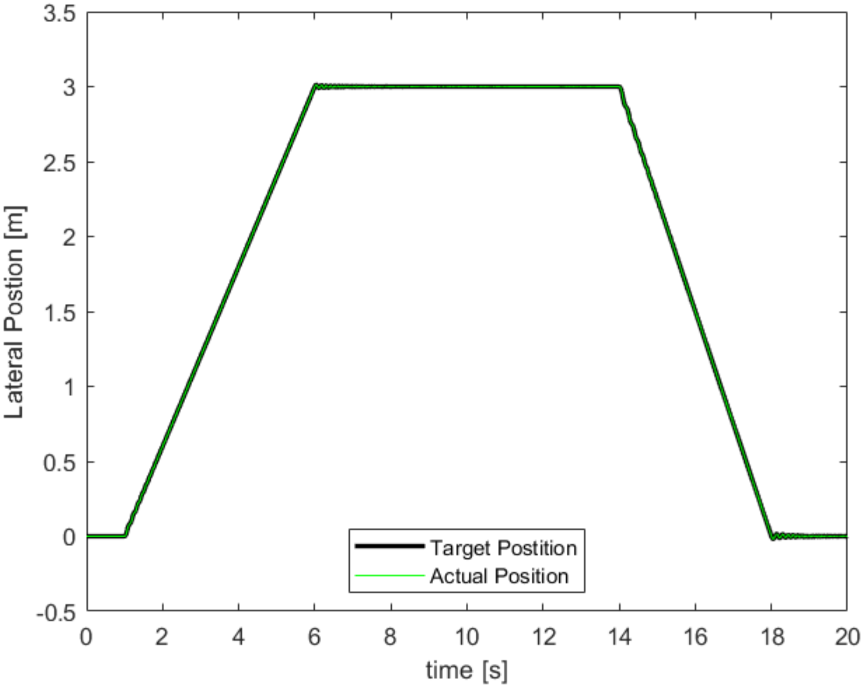

Figure 2.2: Lateral Position Tracking During Double-Lane Change Maneuver

the vehicle's lateral position to begin at $0m$ at simulation start up and remain in that position from t = $0s$ to t = $1s$. From t = $1s$ to t = $6s$, the vehicle moves to a lateral position of $3m$. The vehicle maintains this position from t = $6s$ to t = $14s$. After completing this sequence, the vehicle returns to its original lane by t = $18s$ and remains there for the rest of the simulation. As seen in Fig. 2.2, the vehicle obeys the control law and successfully completes the maneuver.

Fig. 2.3 and Fig. 2.4 depict the yaw-rate tracking and sideslip angle tracking respectively. From these figures, it is apparent that the LQR is bringing these states to their desired values which were created by the human driver MPC.

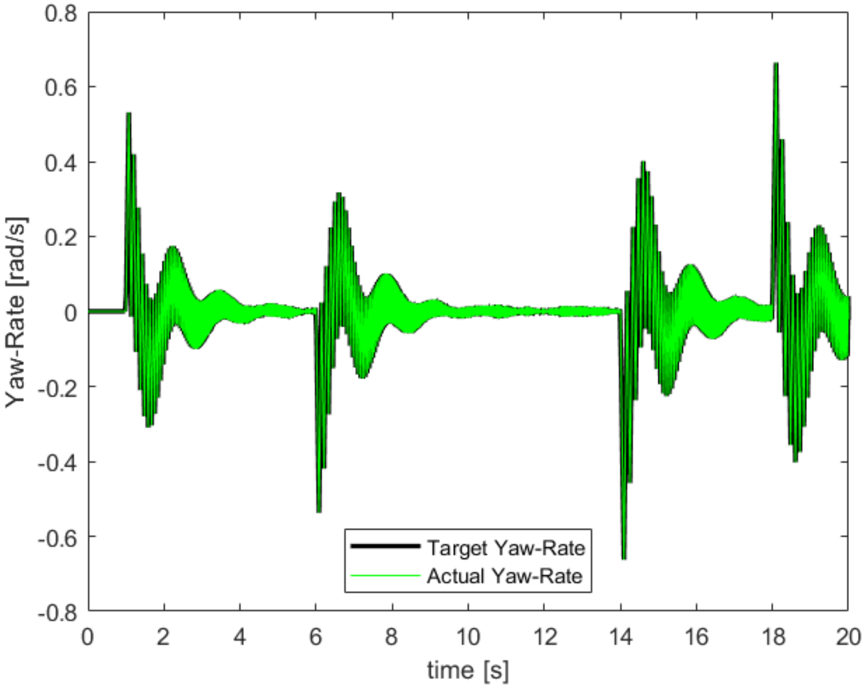

Figure 2.3: Yaw-Rate Tracking During Double-Lane Change Maneuver

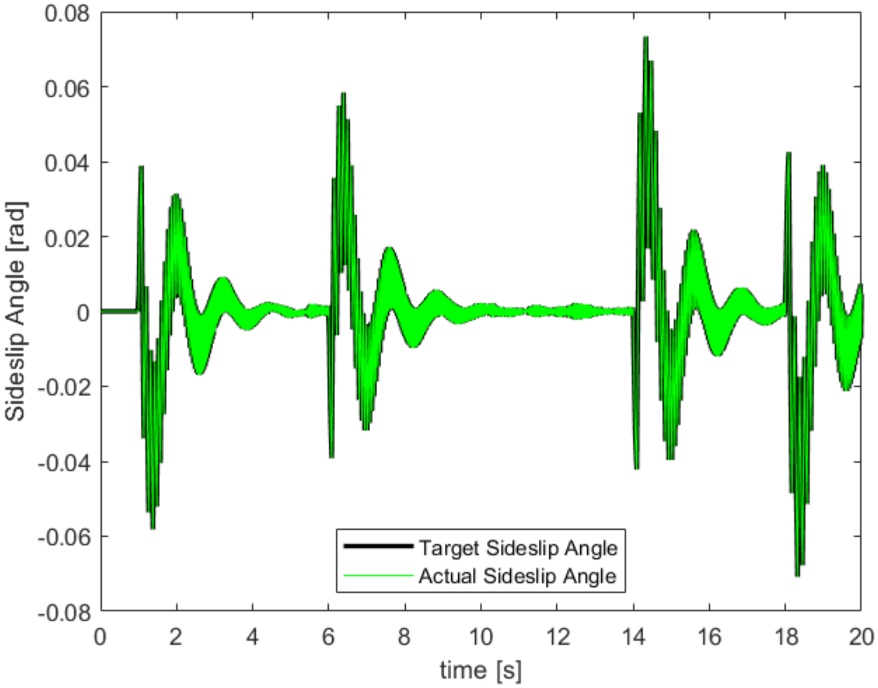

Figure 2.4: Sideslip Angle Tracking During Double-Lane Change Maneuver

Chapter 3

Brushless DC Motor Modeling and Control Scheme

This chapter is devoted to describing the motor-drive system used for this electric vehicle. As mentioned previously, the vehicle at hand uses an independent Brushless DC motor at each wheel, and the motors are controlled by means of Direct Torque Control. The motors used possess a large enough rotational inertia to provide a large enough summed output torque to move the vehicle's mass. Modeling for the Brushless DC machine was completed similarly to what is seen in [37].

3.1 Mechanical Modeling

The mechanics of the machines concern the rotational moment of inertia J, the load torque T_L, the damping force coefficient B, electromagnetic torque T_e, shaft speed ω_r, and shaft angle θ_r. Eq. 3.1 is utilized to solve for the position of the shaft as well as its speed.

$$T_e = J\frac{d\omega_r}{dt} + B\omega_r + T_L \tag{3.1}$$

Eq. 3.1 can be rearranged to solve for the time derivative of shaft speed, and then be integrated once to solve for the shaft speed, and then integrated again to solve for the position of the shaft.

Table 3.1: Converter Voltages and Currents

Switch On	**Current Polarity**	v_{xg}	i_{xdc}
Upper	+	v_{dc}	i_{xs}
	-	$v_{dc} + v_d$	i_{xs}
	0	v_{dc}	i_{xs}
Lower	+	$-v_d$	0
	-	v_{sw}	0
	0	0	0
Neither	+	$-v_d$	0
	-	$v_{dc} + v_d$	i_{xs}
	0	$v_{dc}/2$	0

3.2 Electrical Modeling

For this motor-drive system, a 6-switch, 2-level converter is used. The voltage between an output leg of the converter and the 0 VDC point is dependent upon the switch position of the converter and the current polarity of the respective phase. Voltage values given these conditions are seen in Table 3.1. Each leg in the converter has three possible switch positions. These include the upper switch being closed while the lower switch remains open, the lower switch being closed and the upper switch is open, or each switch being open. Under no circumstances are both switches in the same leg left open.

In Table 3.1, v_{xg} is the voltage between the respective converter leg and 0 VDC. v_{dc} is the DC link voltage, and v_d is the voltage drop across the switch.

After finding the phase to ground voltage of each phase leg, the phase to neutral voltage for each phase must be found. This is accomplished by first finding the neutral to ground voltage. This is given by Eq. 3.2.

$$v_{ng} = \frac{1}{3}(v_{ag} + v_{bg} + v_{cg}) \tag{3.2}$$

The stator voltages are then found using Eq. 3.3.

$$v_{xs} = v_{xg} - v_{ng} \tag{3.3}$$

After finding stator voltages, stator currents can then be solved for. Eq. 3.4 depicts the voltage equations for the stator windings of the machine. Here, r_s is the winding resistance, L_s is the winding inductance, and i_s is the winding current.

$$v_{xs} = r_s * i_x + L_s \frac{di_x}{dt} \tag{3.4}$$

By rearranging Eq. 3.4 into the form of Eq. 3.5, this KVL equation can be used as a solution for current in simulation.

$$i_x = \int \frac{v_{xs} - r_s * i_x}{L_s} \, dt \tag{3.5}$$

In this model, an accurate estimate of electromagnetic torque must be made. The first step for making this estimate involves modeling the back EMF voltages for each of the phases. Here, back-EMF takes on a trapezoidal waveform, and is a function of rotor speed and the trapezoidal function for each phase.

$$E_x = K_e * \omega_r * F_x \tag{3.6}$$

Eq. 3.6 provides the back EMF for each phase, where E_x is the back EMF for an arbitrary phase, K_e is the back EMF constant, and F_x is the trapezoidal function for an arbitrary phase. The torque constant has units Volts per speed and provides the relationship between voltage and shaft speed.

For the trapezoidal back EMF function, each phase is separated by 120 degrees. Fig. 3.4 depicts the nature of each of these functions during a period of constant torque. Eq. 3.7 - Eq. 3.9 depict the piece-wise functions describing each trapezoidal function. Here, it is apparent that back EMF is not only dependent upon shaft speed, but also the position of the shaft.

$$\begin{aligned} F_a(\theta_r) = \quad & \theta_r \frac{6}{\pi}, \ 0 \ \leq \ \theta_r < \frac{\pi}{6} \\ & 1, \ \frac{\pi}{6} \ \leq \theta_r \ < \frac{5\pi}{6} \\ & (\pi - \theta_r)\frac{6}{\pi}, \frac{5\pi}{6} \ \leq \theta_r \ < \frac{7\pi}{6} \\ & -1, \ \frac{7\pi}{6} \ \leq \theta_r < \frac{11\pi}{6} \\ & (\theta_r - 2\pi)\frac{6}{\pi}, \ \frac{11\pi}{6} \leq \theta_r < 2\pi \end{aligned} \tag{3.7}$$

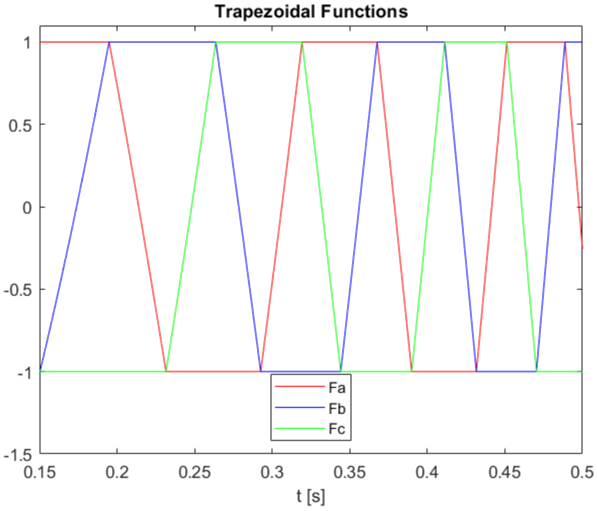

Figure 3.1: Trapezoidal Back EMF Functions

$$
\begin{aligned}
F_b(\theta_r) = \quad & -1,\ 0\ \leq \theta_r < \frac{\pi}{2} \\
(-\frac{2\pi}{3} + \theta_r)\frac{6}{\pi},\ & \frac{\pi}{2} \leq \theta_r < \frac{5\pi}{6} \\
1,\ & \frac{5\pi}{6}\ \leq \theta_r\ \frac{3\pi}{2} \\
(-\frac{5\pi}{3} + \theta_r)\frac{6}{\pi},\ & \frac{3\pi}{2} \leq \theta_r\ < \frac{11\pi}{6} \\
-1,\ & \frac{11\pi}{6}\ \leq \theta_r <\ 2\pi
\end{aligned}
\tag{3.8}
$$

$$
\begin{aligned}
F_c(\theta_r) = \quad & 1,\ 0\ \leq \theta_r < \frac{\pi}{6} \\
(\frac{\pi}{3} - \theta_r)\frac{\pi}{6},\ & \frac{\pi}{6}\ \leq \theta_r < \frac{\pi}{2} \\
-1,\ & \frac{\pi}{2}\ \leq \theta_r < \frac{7\pi}{2} \\
(-\frac{4\pi}{3} + \theta_r)\frac{6}{\pi},\ & \frac{7\pi}{2}\ \leq \theta_r < \frac{3\pi}{2} \\
1,\ & \frac{3\pi}{2}\ \leq \theta_r < 2\pi
\end{aligned}
\tag{3.9}
$$

The next step for making an accurate electromagnetic torque estimation entails solving for the back EMFs in the stationary reference frame as well as the stator winding currents. This is realized utilizing Eq. 3.10 and Eq. 3.11. For balanced systems, such as this, the zero axis components may be neglected since they equal zero.

$$\begin{bmatrix} e_q^s \\ e_d^s \\ e_z^s \end{bmatrix} = \frac{2}{3} \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} e_a \\ e_b \\ e_c \end{bmatrix} \tag{3.10}$$

$$\begin{bmatrix} i_q^s \\ i_d^s \\ i_z^s \end{bmatrix} = \frac{2}{3} \begin{bmatrix} 1 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & -\frac{\sqrt{3}}{2} & \frac{\sqrt{3}}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \end{bmatrix} \begin{bmatrix} i_a \\ i_b \\ i_c \end{bmatrix} \tag{3.11}$$

An estimate for electromagnetic torque can then be made using Eq. 3.12. Note that rotor speed is in the denominator of the equation and that rotor speed is zero at simulation initialization. Therefore, a prime mover is required at the first time step of the simulation.

$$T_e = \frac{E_q^s}{\omega_r} * I_q^s + \frac{E_d^s}{\omega_r} * I_d^s \tag{3.12}$$

3.3 Direct-Torque Control

Unlike many motor control schemes, Direct-Torque Control, DTC aims to directly control the motor's output torque opposed to its shaft speed. For the vehicular system used in this study, each motor receives a torque command from the torque split. These are the target torque outputs. DTC was modeled according to the procedure set in [38].

Significant components for this method include a flux and torque estimator, multiple comparators, a table look up, and sample and hold blocks. Sample and hold blocks are necessary for preventing the switches of the converter from changing too quickly. Therefore, the sample and hold blocks prevent the switches from changing faster than the simulation's time-step. The comparators are utilized to make numerical comparisons between the estimated torque and flux to the desired torque and flux. Two metrics are created for the torque estimation. These include the angle α between the q axis and d axis flux linkage and the vector magnitude of the q axis and d axis flux linkage. The angle α is found by taking the arc tangent between the q axis and d axis flux linkage. The angle α is then utilized to determine which of the 6 sections the flux vector lies in, which is seen in Fig. 3.4. Note that each of these section has a bandwidth of 60 degrees.

Table 3.2: Voltage Vectors and Switching States

Voltage Vector	$T1/\overline{T4}$	$T2/\overline{T5}$	$T3/\overline{T6}$
V_0	0	0	0
V_1	1	0	0
V_2	1	1	0
V_3	0	1	0
V_4	0	1	1
V_5	0	0	1
V_6	1	0	1
V_7	1	1	1

The first part of the process for DTC involves the comparison between desired and requested values for torque and flux. As seen in Fig. 3.2, a boolean decision is made after the comparator's output. The output is reflected in Table 3.3. For ΔT_e, if the difference between requested torque is positive, the variable is set to one, if the difference is negative, the variable is set to negative one, and if the difference is zero (or close to zero), the variable is set to zero. The comparator for flux takes the difference between the requested flux magnitude vector and the estimated flux magnitude vector. Unlike the boolean torque variable, $|\lambda_s|$ can only take on values zero or one. If the difference is large enough, the variable is set to one, and is otherwise set to zero. The possible voltage vectors are seen in Fig. 3.3.

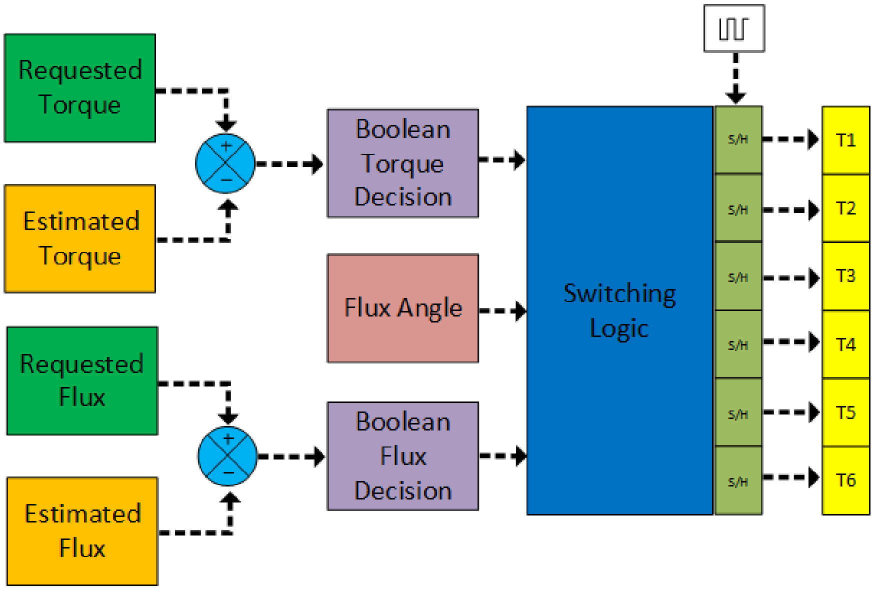

Figure 3.2: DTC Control Diagram

After making a boolean decision for each of the comparator's outputs, a voltage vector must

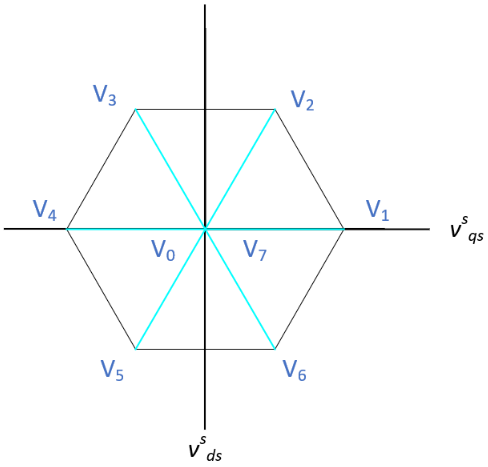

Figure 3.3: Voltage Vector and Switching States

Table 3.3: Switching Table for Direct-Torque Control

ΔT_e	$\Delta\lvert\lambda_s\rvert$	I	II	III	IV	V	VI
1	1	V_2	V_3	V_4	V_5	V_6	V_1
0	1	V_7	V_0	V_7	V_0	V_7	V_0
-1	1	V_6	V_1	V_2	V_3	V_4	V_5
1	0	V_3	V_4	V_5	V_6	V_1	V_2
0	0	V_0	V_7	V_0	V_7	V_0	V_7
-1	0	V_5	V_6	V_1	V_2	V_3	V_4

be applied from the converter to bring both of the boolean variables to zero. In table 3.3, it is seen that there are six possible voltage vectors to execute for each of six possible states of the variables. Which voltage vector is applied is dependent upon the location of angle α as seen in Fig. 3.4. After determining what voltage vector should be applied to machine's stator windings, Table 3.2 is utilized to determine the correct converter switching sequence.

The prowess of DTC for Brushless DC machines is seen in Fig. 3.5. Here, the output torque of the machine accurately tracks the reference step command from 1 Nm of torque to 4 Nm. As seen from the graph, desired torque maintains values centered around the reference.

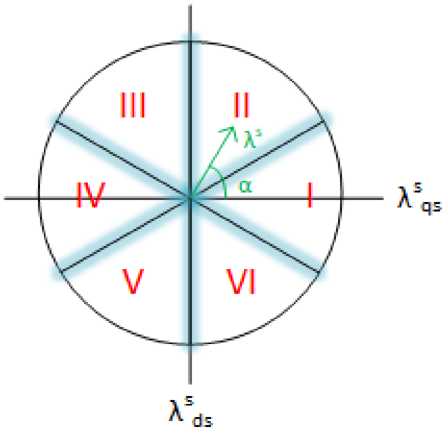

Figure 3.4: Stator Flux Position Graph

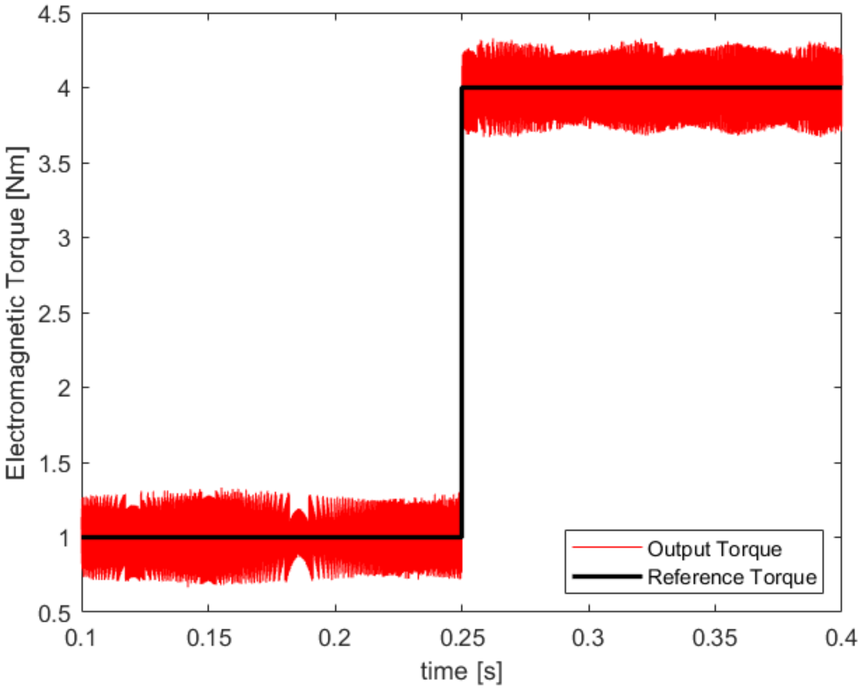

Figure 3.5: DTC Step Response Performance

Chapter 4

Cyber-Attack Modeling and Detection Schemes

In this study, three different forms of cyber-attacks are placed on the vehicle's LSCS. These include Data Integrity Attacks, Replay Attacks, and Denial of Service Attacks. The purpose of the attacks is to distort the sensor value seen in the LSCS and the human driver MPC. This will in turn alter the necessary control action of the LSCS to reach the desired lateral trajectory commands sent from the MPC and will also distort the necessary lateral trajectory commands to accomplish the double-lane change maneuver. Yaw-rate and sideslip angle are the most dynamic signals used by the LSCS, and are therefore the signals placed under cyber-threat.

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

4.1 Data Integrity Attack

Data Integrity Attacks aim to skew the real value of the signal by either scaling the signal by a value other than one, summing the signal with a value other than zero, or using the combination of both methods. Eq. 4.1 and Eq. 4.2 express the nature of this attack in equation form.

$$\gamma_{atck} = v\gamma + \epsilon \tag{4.1}$$

$$\beta_{atck} = v\beta + \epsilon \tag{4.2}$$

As seen from Eq. 4.1 and Eq. 4.2, Data Integrity Attacks linearly corrupt the signal. Epsilon inflicts the same effect on the signal of the attack for the duration of the simulation, and v linearly effects the attack for the duration of the simulation. In this study, the Data Integrity attack lasts from $t = 3s$ to $t = 4s$. The attack is placed during this time frame since the vehicle is making a lateral movement from the starting lane to the next lane.

4.2 Replay Attack

Replay Attacks are another common form of cyber-attacks which effect the true value of a signal. In the event of a Replay Attack, the signal is not allowed to update during the time-steps governed by the attack length. Therefore, the value of the signal at the beginning of the attack will be the same value seen by the LSCS and MPC for the duration of the attack.

$$\gamma_{atck} = \gamma_{t_{start}} \tag{4.3}$$

$$\beta_{atck} = \beta_{t_{start}} \tag{4.4}$$

The effects on the signals seen by the MPC and LSCS can be realized through Eq. 4.3 and Eq. 4.4. Here, t_{start} depicts the signal at the time-step the attack begins. The signal will remain the same until the attack has been removed. In this study, each Replay Attack begins at $t = 3.2s$ and lasts a variable amount of time. The severity of the Replay Attack increases with the duration of the attack.

4.3 Denial of Service Attacks

The Denial of Service, DOS, Attack is another form of cyber-attacks. This form of attack interferes with the sampling of a signal. DOS attacks can be used to either slow down the rate at which a signal is samples, or flood the controller using the signal with updated values for a signal at a rate that is higher than which the controller is designed to sample. There are many different forms of DOS attacks. In [39], Low-Rate DOS Attacks are used to throttle the flow of information between two points of communications. Other forms of DOS attacks are given in [40], and include Application Layer Attacks, Reflection Attacks, Amplification Attacks, and Zero-Day DDoS Attacks.

In this study, DOS attacks are manifested by adjusting the rate at which one of the signals is allowed to update. As an example, if a signal were under a DOS attack, it will be sampled at a different rate than the rest of the system. Therefore, the LSCS and MPC will see different values for the signal at different rates than the signal not under DOS attack.

$$Sample - Time_{\beta} = \frac{1}{m}(time - step), Sample - Time_{\gamma} = time - step \tag{4.5}$$

$$Sample - Time_{\gamma} = \frac{1}{m}(time - step), Sample - Time_{\beta} = time - step \tag{4.6}$$

Eq. 4.5 and Eq. 4.6 govern the time-steps of the simulation in the event of a DOS attack. The time-step altering variable m modifies the jeopardized signal. As is the nature of simulation, the signal can not be updated faster than the predefined time-step of the simulation. Therefore, m decreases the sampling-rate. As an example, using Eq. 4.5, m may be set to 0.5. If this were the case, the sideslip angle signal would only update at half of the rate the yaw-rate would update. In this study, multiple values of m are used and the DOS Attack lasts the entirety of the simulation.

4.4 Detection Method Preface

Cyber-Security requires an accurate understanding of the system at hand under normal operating conditions in order to make an accurate decision as to whether the system studied is facing a cyber-attack. This study incorporates this strategy by first conducting a study under safe conditions and evaluates the lateral metrics of the system in an offline manner.

Here, the vehicle's yaw-rate, and sideslip angle are used to make a cyber-security decision.

Three forms of the lateral metrics are used. They include their actual values, estimated values from the state-space observer, and the predictions made by a pre-trained Neural-Network.

There are three different detection methods utilized to detect the cyber-threat. First, there is a residual metric, DM: 1, which compares actual and estimated values. The second detection method, DM: 2, compares target and estimated values. Lastly, DM: 3, compares the output of the Neural-Network to the observer's estimated values.

While the values used by the detection method's are not the same, the underlying principal of the detection strategy is the same. In this simulation, a fixed time-step of 0.0001 s is used. Prior to implementing a cyber-attack, Eq. 4.10, Eq. 4.11, and Eq. 4.12 are called at each time-step. These can be considered as a form of error. The values gained from these error equations are used to create an error band. The error band serves as a guideline as to suitable error values during normal operation. The error band values can be stored in a vector and read back into the program during simulation. If error metrics excceed the error band plus a predetermined threshold, the system is assumed to be under cyber-attack.

4.5 Residual Metric Comparing Actual and Estimated Lateral Metrics, DM: 1

As stated previously, DM: 1 makes a comparison between the actual and estimated yaw-rate and sideslip angle. Its band is governed by Eq. 4.10. An observer is a useful controls tool, that can make estimates as to the system's states. Observers are often used whenever the states of a given system cannot be measured. Estimated values are found by finding an observer gain L that will make the observer system converge to the actual states. Converging to the actual states is done 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 Eq. 4.7 - Eq. 4.9.

$$A = \begin{bmatrix} A - Bk & Bk \\ zeros(size(A)) & A - LC \end{bmatrix} \tag{4.7}$$

$$B = \begin{bmatrix} B \\ zeros(size(B)) \end{bmatrix} \tag{4.8}$$

$$C = \begin{bmatrix} C & zeros(size(C)) \end{bmatrix} \tag{4.9}$$

In Eq. 4.10, $\beta(i)$ and $\gamma(i)$ represent actual lateral values discovered through the LSCS, whereas $\beta_{est}(i)$ and $\gamma_{est}(i)$ depict the estimated metrics found through the observer. As seen from Eq. 4.10, r_1 takes on the sum of the differences between estimated and actual lateral values for 10 time steps to create the band.

$$r_1 = \sum_{i=1}^{10} (\beta(i) - \beta_{est}(i))^2 + (\gamma(i) - \gamma_{est}(i))^2 \tag{4.10}$$

Fig. 5.2 depicts the residual band for DM: 1, as well as the output of Eq. 4.10 at each time step. Note, that the residual band has also been summed with a predefined threshold.

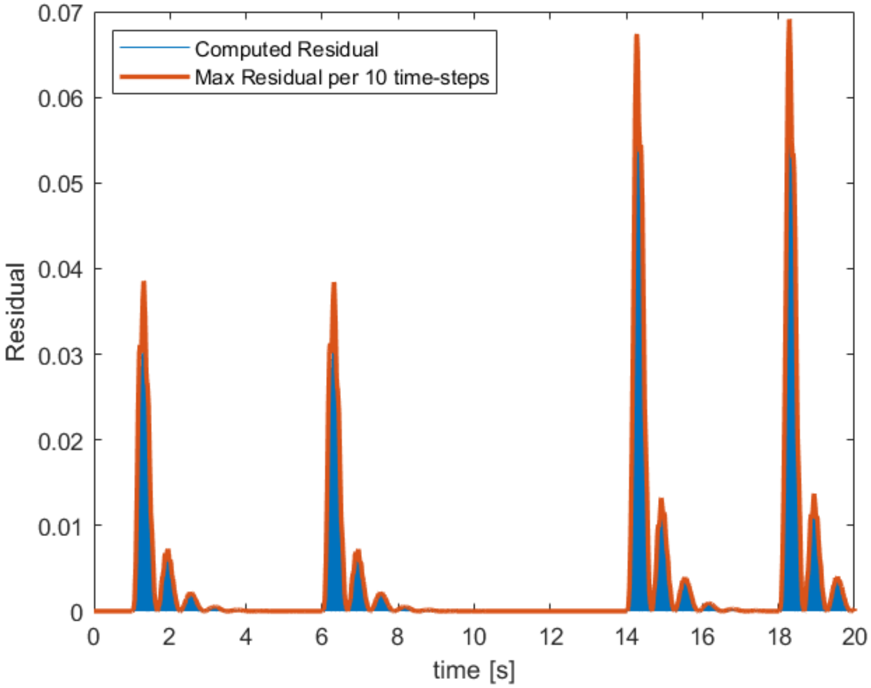

Figure 4.1: Residual Metric for Actual and Estimated Values

4.6 Residual Metric Comparing Target and Estimated Metrics, DM: 2

DM: 2 is the second detection scheme used in this study, and makes the comparison between the target yaw-rate and sideslip angle (discovered through the MPC), and the estimated lateral metrics discussed previously. It is interesting to note that the peaks in r_2 have a larger magnitude than those of r_1. The reason this occurs is related to the nature of the lateral values at time step they are associated with. In Eq. 4.11, $\gamma_{tar}(i)$ and $\beta_{tar}(i)$ provide the target values of sideslip angle and yaw-rate which minimize the difference between actual and target lateral position of the vehicle at the next time-step. Therefore, the target values deal with the system placed one time-step into the future in comparison to the estimated values. Fig. 4.2 displays the graph for r_2.

$$r_2 = \sum_{i=1}^{10} (\beta_{tar}(i) - \beta_{est}(i))^2 + (\gamma_{tar}(i) - \gamma_{est}(i))^2 \tag{4.11}$$

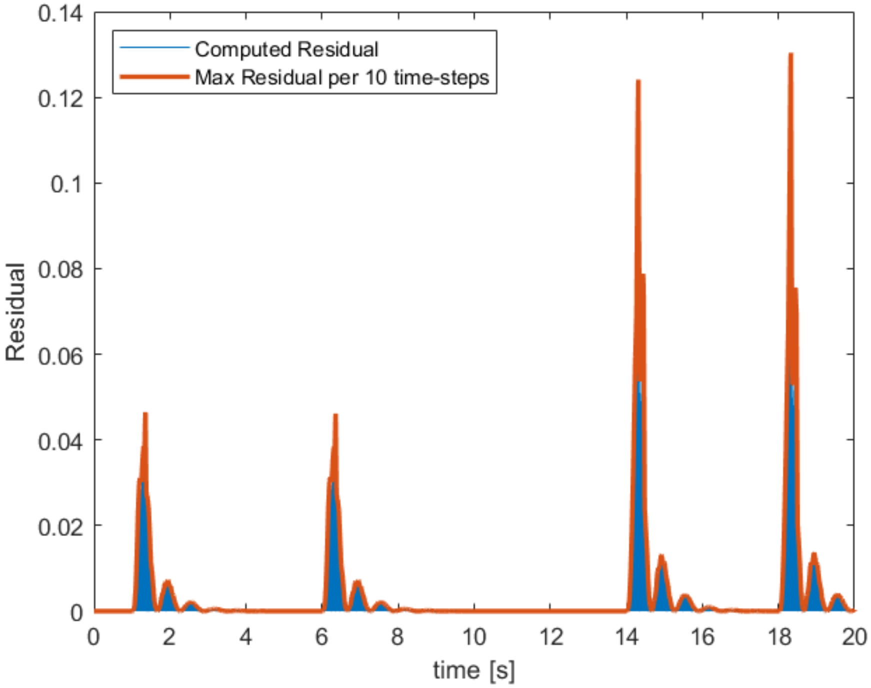

Figure 4.2: Residual Metric for Estimated and Target Values

4.7 Residual Metric Comparing Neural-Network Output to Estimated Metrics, DM: 3

Neural-Networks are well suited for making accurate predictions, given the model was trained using a robust data set. For the problem at hand, a Neural-Network is an appropriate tool for making predictions as to the vehicle's yaw-rate and sideslip angle at the current time-step. A Neural-Network model was created utilizing MATLAB Simulink's Deep Learning Tool Box. A training data set was created offline using various drive cycles that did not include the actual lateral movement used in the cyber-security study. The Levenberg-Marquardt optimization tool was used to train the network. This training strategy is responsible for modifying the Neural-Network's weights and biases at each epoch that will minimize the error gradient. According to Mathwork's documentation regarding the algorithm, it is considered to be one of the fastest algorithms in terms of convergence time.

A depiction of the model is made by Fig. 4.3. As seen by the figure, the model takes on four different inputs. These include the actual yaw-rate and sideslip angle of the system at the previous time-step, as well as the target yaw-rate and sideslip angle at the previous time-step. These inputs are passed through the Neural-Network model and create two distinct outputs. These include the predicted sideslip angle and yaw-rate at the current time-step.

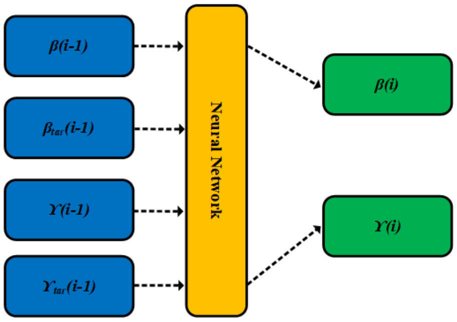

Figure 4.3: Neural-Network Architecture

$$r_3 = \sum_{i=1}^{10} (\beta_{NN}(i) - \beta_{est}(i))^2 + (\gamma_{NN}(i) - \gamma_{est}(i))^2 \tag{4.12}$$

In Eq. 4.12, $\beta_{NN}(i)$ and $\gamma_{NN}(i)$ represent the output of the Neural-Network. These metrics are compared with the output of the observer to manifest the residual band for DM: 3. Fig. 4.4

illustrates this residual band.

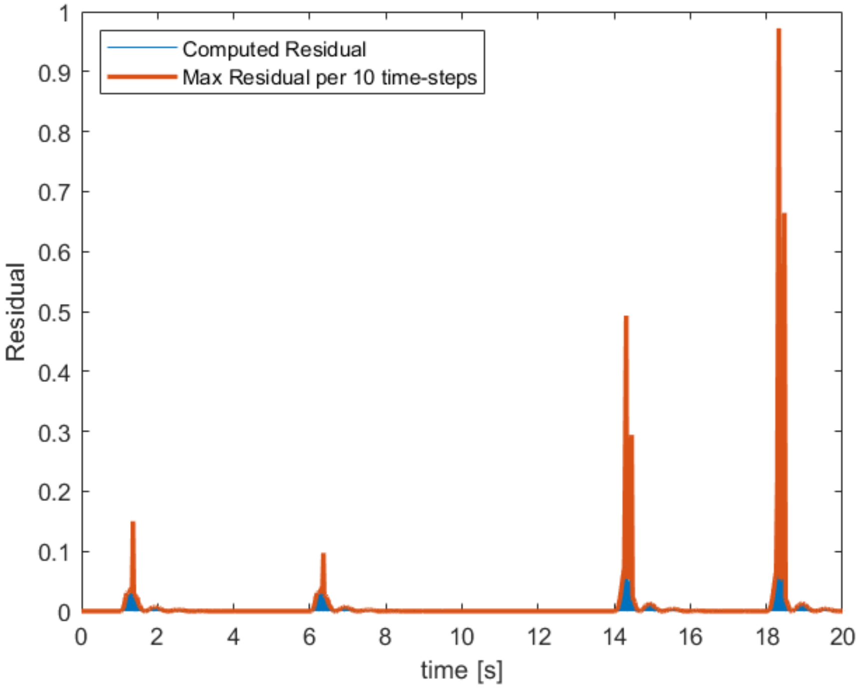

Figure 4.4: Residual Metric for NN and Estimated Values

Chapter 5

Results and Analysis

The purpose of this chapter is to illustrate the effectiveness of each of the three detection schemes for making cyber-threat defections in the event of each of the cyber-attack schemes described previously. This chapter begins by displaying graphical information to visually describe at what point in the simulation the attacks were or were not detected, and comparing the detective prowess of each method. Note that in Chapter 5, a filled in circle represent the successful detection of a cyber-attack, and a blank circle depicts the failure of an attack.

5.1 Performance seen through Graphics

The first attack studied is a Data Integrity Attack, where the nature of the attack involves scaling the true value of the signal with a value other than one. As seen in Fig. 5.1, six different values of m are utilized. The values of m include 0, 0.5, 0.9, 1.01, 1.1, and 1.5. Obviously, values that stray farther from one have a larger impact on signal distortion.

Fig. 5.1 shows that different detection methods performed differently depending upon whether yaw-rate or sideslip angle was being targeted. In the case of yaw-rate being placed under attack, DM: 1 exhibited superior performance to its counterparts. For three of the six attack forms, it was able to detect the attack within the first two time-steps. In contrast, for the attack targeting the sideslip angle sensor, DM: 3 was able to detect five of the six attacks. DM: 3 was also the only one of the three detection schemes capable of noticing the presence of an attack for an m value of 1.1.

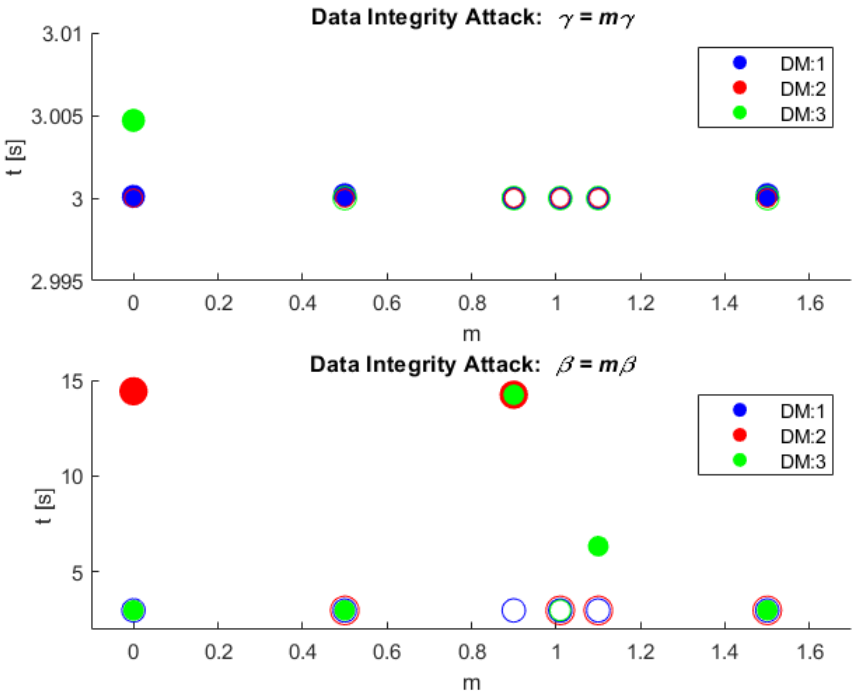

Figure 5.1: Data Integrity Attack Detection Times

Fig. 5.2 depicts Data Integrity Attacks where the true value of a signal is summed with a value other than zero over the duration of the attack. In this scheme, m takes on value that are either positive or negative, and it is clear that the potency of the attack is dependent upon the size of the magnitude of the attack signal. Values for m include $\pm 0.1, 0.01, 0.001$. For this form of a Data Integrity Attacks targeting the yaw-rate, each detection method provided similar results. For m values of ± 0.1, each detection method was able to detect the attack. DM: 1 provided the quickest response for detecting the attack, with DM: 3 being the second fastest. All three detection methods were unable to discern the attacks of the four smallest magnitudes. When sideslip angle faces this form of attack, DM: 3 provided a 100% detection rate. Note that detection occurs outside the range of attack. This is not caused by the accruing residual, since the residual is reset to zero at the end of every 10 time-steps. This is caused by by the permanent effects placed on the vehicle during lateral movements. While the vehicle still completes the maneuver, lateral metrics are altered from the offline simulation, causing distinct differences in the vehicle's movements later in the simulation. These changes are noticed once the vehicle is making the return to its original lane.

Fig. 5.3 illustrates the performance statistics of each of the detection methods when the

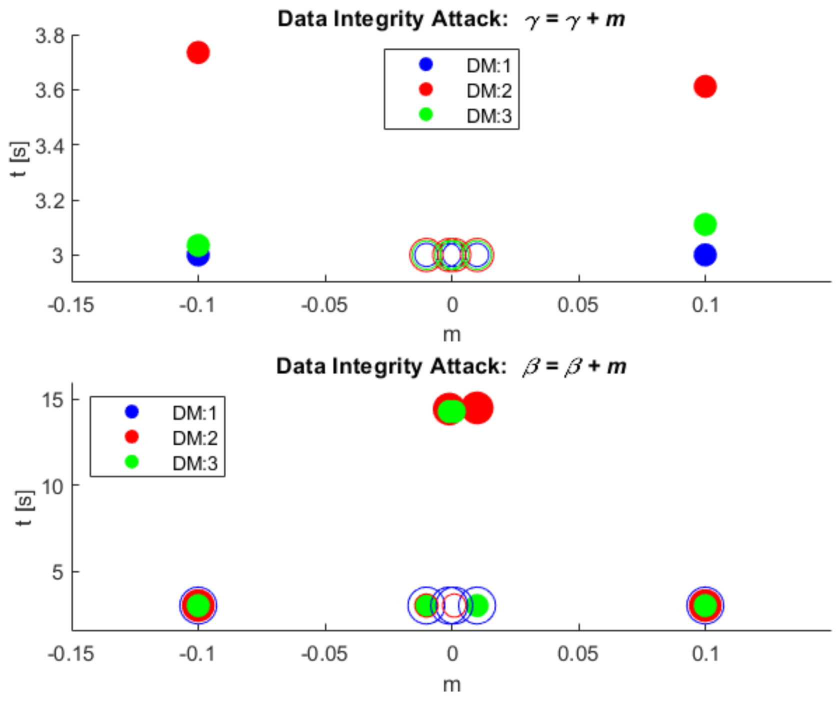

Figure 5.2: Data Integrity Attack Detection Time Statistics

vehicle is placed under a Replay Attack. As described previously in this study, the Replay Attack is initiated at $t = 3.2s$. The severity of the attack is dependent upon the longevity of the attack. Attack lengths include 0.05, 0.1, 0.3, 0.4, and 0.5 s. When the replay attack is focused on the yaw-rate sensor, DM: 1 outperforms DM: 2 and DM: 3 in terms of detection rate and detection time. For each length of attack, DM: 1 makes a successful detection at the same time-step. DM: 3 catches three of the five attack scenarios and DM: 2 misses each attack.

As discussed previously, DOS Attacks target the sampling rate of a signal. Here, the DOS Attack only allows a targeted signal to update at a rate that is different from other sensor signals. Fig. 5.4 depicts each detection method's performance for when a signal is only allowed to update every two time-steps, and when a signal is only allowed to update every three time-steps. In the first case, where sideslip angle updates slower than yaw-rate, DM: 1 is the only detection method unable to detect the cyber-attack. DM: 2 and DM: 3 make a successful detection, but DM: 3 detects the attack over twice as fast. Whenever the yaw-rate is sampled at a smaller rate than sideslip angle, each of the detection methods notify the presence of an attack, but DM: 3 provides the fastest response.

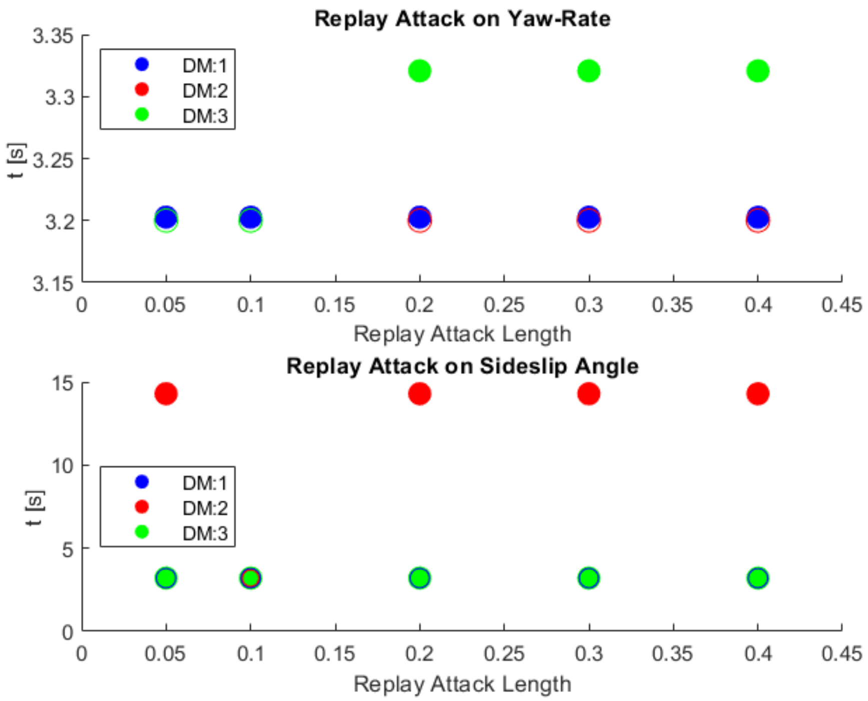

Figure 5.3: Replay Attack Detection Time Statistics

5.2 Performance seen through Numerical Comparison

This section is utilized to make a numerical comparison between respective detection method's performance on detecting the cyber-threats and to make a reasonable argument as to which of the three methods provides the most security. This method not only distinguishes whether or not a detection was made, but also the amount of time it takes for the detection method to detect the attack after the attack has been initiated.

To start, the attack data must first be prepared in a way that allows attack data across all forms of attacks to be compared to each other. The data preparation process can be most easily understood through the flowchart seen in Fig. 5.5. Note that the logic seen in this flowchart must be executed once for each of the detection methods.

The process begins by setting two counter variables, (i, j), equal to one. Storage variables, s_γ and s_β are set equal to zero. The variable i represents the quantity of subsets of one of the forms of the four attacks. As an example, the summation Data-Integrity Attack would have five values for i. These include the five values of m used in the attack. While in the first loop, s_γ and s_β are

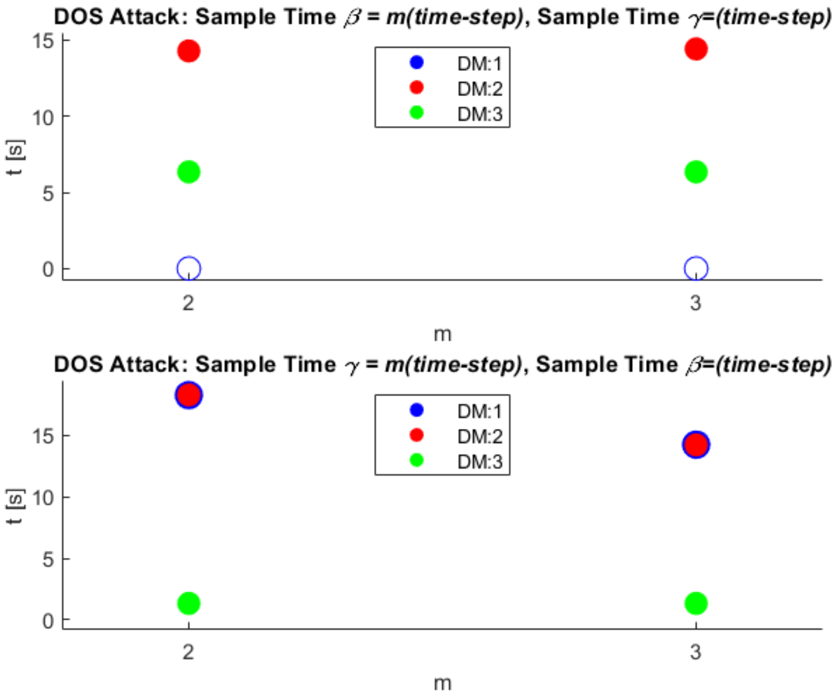

Figure 5.4: DOS Attack Detection Time Statistics

Table 5.1: Detection Method Score

Detection Method	*Score*
$DM:1$	4.8482
$DM:2$	6.6022
$DM:3$	2.9199

summed with themselves, and the difference between detection time and attack. In the event that a detection method missed the presence of an attack, the end of simulation time, ($t = 20s$), is used. Upon completion of the first loop, the summed values of s_γ and s_β are passed to a vector of size $2 * j = 8$. At the end of the data preparation, there are three vectors of size eight, unique to the respective detection method. The data set can now be normalized by means of Eq. 5.1. Elements of each vector describing the respective detection methods can be summed. The summed value is then used as a numeric score. As seen from Table 5.1, DM: 3 provided the best score making it the most suitable method for detecting cyber-threats.

$$S_{DM:x} = \frac{S_{DM:x} - S_{DM:xmin}}{S_{DM:xmax} - S_{DM:xmin}} \tag{5.1}$$

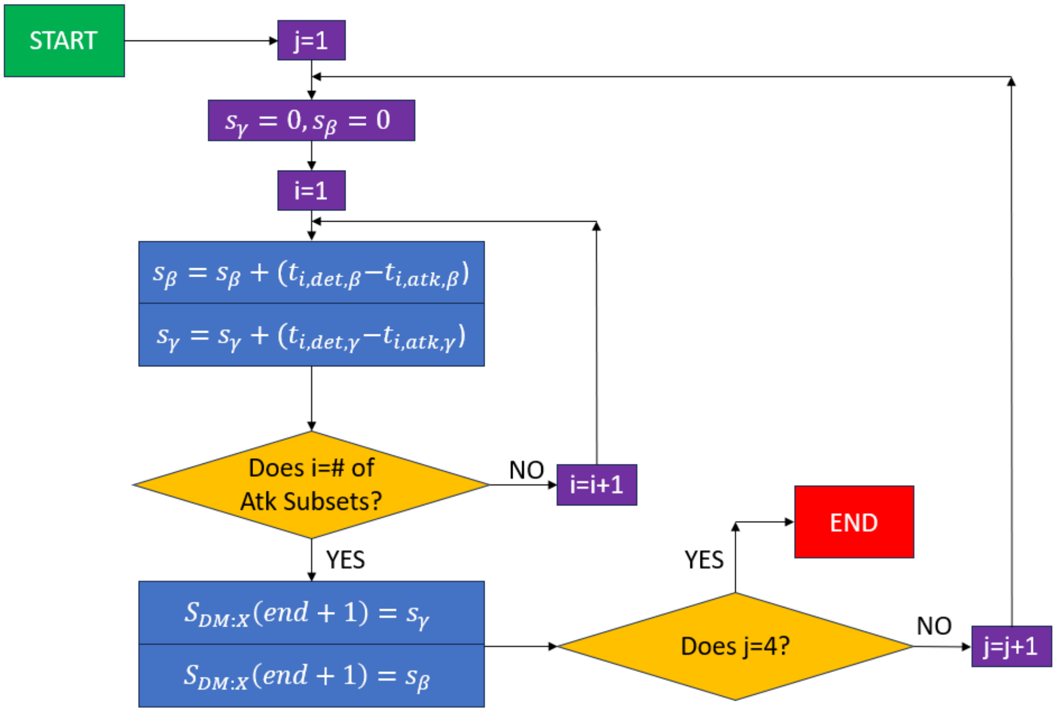
START
j=1
$s_\gamma = 0, s_\beta = 0$
i=1
$s_\beta = s_\beta + (t_{i,det,\beta} - t_{i,atk,\beta})$
$s_\gamma = s_\gamma + (t_{i,det,\gamma} - t_{i,atk,\gamma})$
Does i=# of Atk Subsets?
NO
i=i+1
YES
$S_{DM:X}(end + 1) = s_\gamma$
$S_{DM:X}(end + 1) = s_\beta$
Does j=4?
YES
END
NO
j=j+1

Figure 5.5: Flowchart Describing Data Preparation Process for Numerical Comparison

Chapter 6

Conclusions and Discussion

6.1 Answering the Research Questions

This thesis presents a comprehensive cyber-security study in an electric vehicle's lateral stability control system. The first step to conducting this study involved the modeling of a four motor-drive electric vehicle that is autonomously controlled. As described in this paper, the vehicle model is controlled through multiple layers of control. The most outer layer of control implements Model Predictive Control to determine what lateral metrics bring the vehicle closest to a desired lateral location. Next, a linear quadratic regulator is utilized to bring the lateral metrics to their reference values. Finally, the additional yaw-moment discerned by the linear quadratic regulator is used in conjunction with a torque split to determine what are the necessary torques at each of the vehicle's wheels. In addition to a sophisticated vehicle model, an appropriate motor drive system was also created that uses Brushless DC motors that are controlled by means of Direct-Torque Control.

Upon completing a dynamic vehicle model, a cyber-security study was conducted. In this study, the vehicle was placed under Data-Integrity Attacks, Replay Attacks, and Denial of Service Attacks. To detect the presence of a cyber-attack, three different threat detection methods were developed. Each detection method uses some combination of sensor data, the estimated values of an observer, and a Neural-Network. Conclusive results drawn from the study indicate that each method provides sound cyber-security for an electric vehicle.

6.2 Recommendations for Further Research

To accommodate the increase of intelligent transportation and infrastructure, a motivated pursuit of research in this field must be continuously developed. For this unique study, there are multiple aspects of the cyber-security portion that can be built upon. At the forefront, a more sophisticated residual could be developed. An idea for this would be to take the current residual bands as a starting point, but device an adaptive band for the residual to take on dynamic environmental variables. These would include variables such as weather fluctuations as well as motor-drive wear and tear. In addition to an adaptive residual band, an artificial intelligence architecture could be developed that prevents the need for an offline band calculation. An example of such architecture would be one that takes on vehicle metrics from previous time-steps, and makes accurate predictions as to the metrics a set amount of time-steps into the future. The future time-step predictions could then be used to manifest residual band.

Appendices

Appendix A MATLAB LQR Coding

Appendix A present coding information for finding the gain matrix K, and creating the observer.

```
Q = [500 0; 0 5000];
R = 1;
K = lqr(A,B,Q,R);
p1=-2.2061 + 1.7499i;
p2=-2.2061 - 1.7499i;
k = place(A,B,[p1 p2]);
o1 = -2.2061*5 + 1.7499i;
o2 = -2.2061*5 - 1.7499i;
C = [1 0; 0 1]
L = place(A’,C’,[o1 o2])’;
```

Bibliography

[1] "The increasing need for electric vehicle cyber-security." `https://upstream.auto/blog/the-hidden-cyber-risks-of-electric-vehicles/`. Accessed: 20223-11-1.

[2] H. Van Den Brink and P. Broos, "Cyber security challenges in the electric vehicle infrastructure," in *CIRED Porto Workshop 2022: E-mobility and power distribution systems*, vol. 2022, pp. 429–432, 2022.

[3] Z. Pourmirza and S. Walker, "Electric vehicle charging station: Cyber security challenges and perspective," in *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, pp. 111–116, 2021.

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

[5] A. Ahalawat, S. Adepu, and J. Gardiner, "Security threats in electric vehicle charging," in *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 399–404, 2022.

[6] S. Saadat, S. Maingot, and S. Bahizad, "Electric vehicle charging station security enhancement measures," in *2020 5th IEEE Workshop on the Electronic Grid (eGRID)*, pp. 1–8, 2020.

[7] R. P. Parameswarath, N. Venkata Abhishek, and B. Sikdar, "Prevent: A mechanism for preventing message tampering attacks in electric vehicle networks," in *2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring)*, pp. 1–5, 2023.

[8] A. Sanghvi and T. Markel, "Cybersecurity for electric vehicle fast-charging infrastructure," in *2021 IEEE Transportation Electrification Conference Expo (ITEC)*, pp. 573–576, 2021.

[9] "This bluetooth attack can steal a tesla model x in minutes." `https://www.wired.com/story/tesla-model-x-hack-bluetooth/`. Accessed: 20223-11-1.

[10] "Hackers remotely kill a jeep on the highway—with me in it." `https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/`. Accessed: 20223-11-1.

[11] "Cyber attacks in connected cars-what tesla did differently to win." `https://www.appknox.com/blog/cyber-attacks-in-connected-cars#:~:text=Having%20said%20that%2C%20as%20a,to%20all%20of%20their%20cars`. Accessed: 20223-11-1.

[12] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song, "Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, vol. 9, no. 4, pp. 4639–4657, 2021.

[13] L. Guo, J. Ye, and L. Du, “Cyber–physical security of energy-efficient powertrain system in hybrid electric vehicles against sophisticated cyberattacks,” *IEEE Transactions on Transportation Electrification*, vol. 7, no. 2, pp. 636–648, 2021.

[14] 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 Transactions on Industrial Informatics*, vol. 17, no. 5, pp. 3335–3347, 2021.

[15] A. Al Mamun, M. Abdullah Al Mamun, and A. Shikfa, “Challenges and mitigation of cyber threat in automated vehicle: An integrated approach,” in *2018 International Conference of Electrical and Electronic Technologies for Automotive*, pp. 1–6, 2018.

[16] L. Guo, B. Yang, and J. Ye, “Enhanced cyber-physical security of steering stability control system for four-wheel independent drive electric vehicles,” in *2020 IEEE Transportation Electrification Conference Expo (ITEC)*, pp. 1240–1245, 2020.

[17] “Yaw rate sensor — standard.” `https://www.standardbrand.com/en/products/sensors/sensors/yaw-rate-sensors#:~:text=A%20Yaw%20Rate%20Sensor%20(or,or%20threatens%20to%20roll%2Dover.` Accessed: 20223-11-1.

[18] H. Grip, L. Imsland, T. Johansen, J. Kalkkuhl, and A. Suissa, “Vehicle sideslip estimation design, implementation, and experimental validation,” *IEEE Control Systems Magazine*, vol. 29, pp. 36–52, 01 2009.

[19] B. Boada, M. Boada, and V. Diaz, “Vehicle sideslip angle measurement based on sensor data fusion using an integrated anfis and an unscented kalman filter algorithm,” *Mechanical Systems and Signal Processing*, vol. 72-73, pp. 832–845, 2016.

[20] J. Liu, Z. Wang, L. Zhang, and P. Walker, “Sideslip angle estimation of ground vehicles: a comparative study,” *IET Control Theory & Applications*, vol. 14, no. 20, pp. 3490–3505, 2020.

[21] C. Li, Y. F. Xie, G. Wang, X. F. Zeng, and H. Jing, “Lateral stability regulation of intelligent electric vehicle based on model predictive control,” *Journal of Intelligent and Connected Vehicles*, vol. 4, no. 3, pp. 104–114, 2021.

[22] Z. Li, P. Wang, H. Liu, Y. Hu, and H. Chen, “Coordinated longitudinal and lateral vehicle stability control based on the combined-slip tire model in the mpc framework,” *Mechanical Systems and Signal Processing*, vol. 161, p. 107947, 2021.

[23] Y. Guo, H. Guo, Z. Yin, M. Cui, and H. Chen, “Vehicle lateral stability controller design for critical running conditions using nmpc based on vehicle dynamics safety envelope,” in *2019 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–8, 2019.

[24] Z. Li, H. Chen, H. Liu, P. Wang, and X. Gong, “Integrated longitudinal and lateral vehicle stability control for extreme conditions with safety dynamic requirements analysis,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 10, pp. 19285–19298, 2022.

[25] J. Zhang and H. Zhang, “Vehicle lateral stability control based on single neuron network,” in *2010 Chinese Control and Decision Conference*, pp. 290–293, 2010.

[26] A. A. Ahmed and A. Saleh Alshandoli, “Using of neural network controller and fuzzy pid control to improve electric vehicle stability based on a14-dof model,” in *2020 International Conference on Electrical Engineering (ICEE)*, pp. 1–6, 2020.

[27] M. Yildirim, M. Polat, and H. Kürüm, “A survey on comparison of electric motor types and drives used for electric vehicles,” in *2014 16th International Power Electronics and Motion Control Conference and Exposition*, pp. 218–223, 2014.

[28] N. Hashemnia and B. Asaei, “Comparative study of using different electric motors in the electric vehicles,” in *2008 18th International Conference on Electrical Machines*, pp. 1–5, 2008.

[29] A. Nikam and H. T. Jadhav, “Modelling simulation of three phases bldc motor for electric braking,” in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1, pp. 540–544, 2019.

[30] S. Jain, M. Israr, and P. Samuel, “Closed loop control of brushless dc motor by various controllers for lightweight evs,” in *2023 5th International Conference on Power, Control Embedded Systems (ICPCES)*, pp. 1–6, 2023.

[31] M. A. Hassanin, F. E. Abdel-Kader, S. I. Amer, and A. E. Abu-Moubarka, “Operation of brushless dc motor to drive the electric vehicle,” in *2018 Twentieth International Middle East Power Systems Conference (MEPCON)*, pp. 500–503, 2018.

[32] M. L. De Klerk and A. K. Saha, “A comprehensive review of advanced traction motor control techniques suitable for electric vehicle applications,” *IEEE Access*, vol. 9, pp. 125080–125108, 2021.

[33] B. Singh, P. Jain, A. Mittal, and J. Gupta, “Direct torque control: a practical approach to electric vehicle,” in *2006 IEEE Power India Conference*, pp. 4 pp.–, 2006.

[34] S. Thangalakshmi, M. Padmarasan, V. Sridevi, and K. S. Kavitha Kumari, “Direct torque controlled induction motor drive for electric vehicles application,” in *2023 8th International Conference on Communication and Electronics Systems (ICCES)*, pp. 204–209, 2023.

[35] R. Morales-Caporal, M. E. Leal-López, J. de Jesús Rangel-Magdaleno, O. Sandre-Hernández, and I. Cruz-Vega, “Direct torque control of a pmsm-drive for electric vehicle applications,” in *2018 International Conference on Electronics, Communications and Computers (CONIELECOMP)*, pp. 232–237, 2018.

[36] L. Guo and J. Ye, “Cyber-physical security of electric vehicles with four motor drives,” *IEEE Transactions on Power Electronics*, vol. 36, no. 4, pp. 4463–4477, 2021.

[37] S.Rambabu, “Modeling and control of a brushless dc motor,” 2007.

[38] P. C. Krause, O. Wasynczuk, S. D. Sudhoff, and S. D. Pekarek, *Analysis of Electric Machinery and Drive Systems*, vol. 75. John Wiley & Sons, 2013.

[39] W. Zhijun, L. Wenjing, L. Liang, and Y. Meng, “Low-rate dos attacks, detection, defense, and challenges: A survey,” *IEEE Access*, vol. 8, pp. 43920–43943, 2020.

[40] M. Afzaal, “An overview of defense techniques against dos attacks,” in *2022 9th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, pp. 1–8, 2022.