2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

Path-Following Control of Autonomous Vehicles under Sensor Attacks*

Muhammad Hilmi[1], Augie Widyotriatmo[1], Ivan Kuncara[2], Yul Yunazwin Nazaruddin[1], and Agus Hasan[3]

Abstract— **This paper addresses a problem related to sensor attacks in autonomous vehicles. We proposes an approach that integrates a path following control framework with a novel nonlinear observer design in the context of autonomous vehicle systems. This tailored approach aims to effectively detect and mitigate sensor attacks, ensuring stable path tracking in the context of path-following dynamics. By leveraging the proposed observer's capabilities, we accurately estimate both the state and magnitude of the attacks. Through a comprehensive series of simulation studies, we demonstrate the practicality and effectiveness of our proposed methodology in enhancing the resilience of autonomous systems against sensor attacks.**

I. INTRODUCTION

In recent years, autonomous systems have emerged as transformative technologies, with wide-reaching impacts across various industries, including transportation [1], energy [2], manufacturing [3], healthcare [4], and agriculture [5]. These systems, driven by sophisticated algorithms, sensors, and machine learning, hold the potential to enhance efficiency, safety, and convenience in a myriad of applications. For instance, in the domain of transportation, autonomous vehicles stand to revolutionize the way we commute, offering the promise of reduced accidents, alleviated traffic congestion, and a re-imagined approach to personal mobility. However, as these autonomous systems become increasingly integrated into our daily lives, vulnerabilities emerge. One pressing concern is the risk of cyber attacks targeting these systems, with potentially severe consequences [6].

In the context of autonomous systems, particularly in safety-critical domains such as autonomous vehicles, cyber attacks fall into two distinct categories [7]. Active attacks involve purposeful actions aimed at disrupting the operation of autonomous systems and encompass techniques like denial-of-service (DoS), jamming, and spoofing [8]. For instance, a DoS attack entails overwhelming a system with an excessive volume of requests, rendering it unresponsive or entirely inaccessible [9]. Jamming attacks, on the other hand, disrupt communication signals among various system components, potentially leading to the misinterpretation or loss of vital data [10]. Meanwhile, spoofing attacks involve falsifying information to deceive the autonomous system [11]. In contrast, passive attacks are characterized by covert operations aimed at discreetly collecting sensitive information without immediate disruption. Espionage attacks fall under this category, typically involving infiltration into the system to gather data regarding its operations.

Effectively countering the challenges posed by sensor attacks in autonomous systems demands a diverse set of strategies. One prevalent approach shies away from relying on predefined mathematical or system models, emphasizing data-driven techniques, anomaly detection, and statistical analysis to identify sensor attacks by recognizing patterns or anomalies in the data. This category includes notable works employing deep learning in neural networks (NN) [12], reinforcement learning applied to autonomous agents [13], convolutional neural networks (CNN), and recurrent neural networks (RNN) [14], notably in the form of long short-term memory (LSTM) [15], for the detection and identification of sensor attacks. These approaches exhibit the potential to effectively detect attacks but are challenged by their inherent complexities, reliance on data quality, and the need for continuous adaptation in dynamic environments.

Conversely, another approach leverages mathematical models and system-level analysis to detect and mitigate sensor attacks effectively. This approach utilizes mathematical algorithms and system dynamics to model normal system behavior and deviations induced by attacks. Notable approaches in this category include methods such as secure state estimation using satisfiability modulo theory (SMT) [16], extended Kalman filters (EKF) [17], adaptive observer [18], as well as statistical approaches like recursive least square optimization [19] and filtering based on variance-constrained distribution [20]. However, it's worth noting that the recursive algorithms involved in sensor attack estimation require relatively substantial memory resources and computational power to function effectively.

This paper introduces a secure state estimation approach utilizing nonlinear observers to detect and estimate sensor attacks within autonomous systems. By harnessing the system's inherent nonlinear dynamics, this approach not only identifies anomalies but also accurately assesses the nature and magnitude of sensor attacks, all while maintaining efficiency with minimal computational demands. The application of nonlinear observers ensures that the control of autonomous systems functions as intended, safeguarding safety and performance even when confronted with adversarial actions. In this paper, we focus on investigating the practical implementation of the proposed nonlinear observer method for detecting and estimating sensor attacks within the context of path following control for autonomous vehicles.

*This work was supported by Institut Teknologi Bandung

[1]M. Hilmi, A. Widyotriatmo, and Y. Yunazwin Nazaruddin are affiliated with Instrumentation and Control Research Group, Bandung Institute of Technology, Bandung 40132, Indonesia muhilmi1999@gmail.com, augie@itb.ac.id, and yul@itb.ac.id

[2]I. Kuncara is affiliated with School of Mechanical Engineering, Chonnam National University, Gwangju 61186, South Korea ivankuncara@jnu.ac.kr

[3]A. Hasan is affiliated with Department of ICT and Natural Sciences, Norwegian University of Science and Technology, Alesund 6009, Norway agus.hasan@ntnu.no

The paper is structured as follows: Section I introduces the topic, emphasizing the importance of autonomous systems and the risks associated with sensor attacks. Section II delves into problem formulation, presenting the autonomous system model and state space formulation. In Section III, the paper covers control and observer design techniques. Section IV presents results from numerical simulations. Finally, in Section V, the paper concludes by summarizing the findings and the performance on detection and estimation of sensor attacks in path following control application of autonomous vehicles.

II. PROBLEM FORMULATION

A. Autonomous System Model

The focus of this study is on the autonomous ground vehicle, depicted as a car-like model in Fig. 1. A car-like vehicle model provides a simplified mathematical representation of a vehicle's motion, commonly employed in the fields of robotics, control systems, and autonomous vehicle navigation. The length of the vehicle (l) is measured from the steering axle to the rear axle. The configuration states of the vehicle are represented by $\begin{bmatrix} x(t) & y(t) & \phi(t) \end{bmatrix}^\intercal$ where $x(t)$ and $y(t)$ represent the positions at time t in the Cartesian coordinates and the orientation relative to these coordinates at time t is denoted as $\phi(t)$, obtained through sensors.

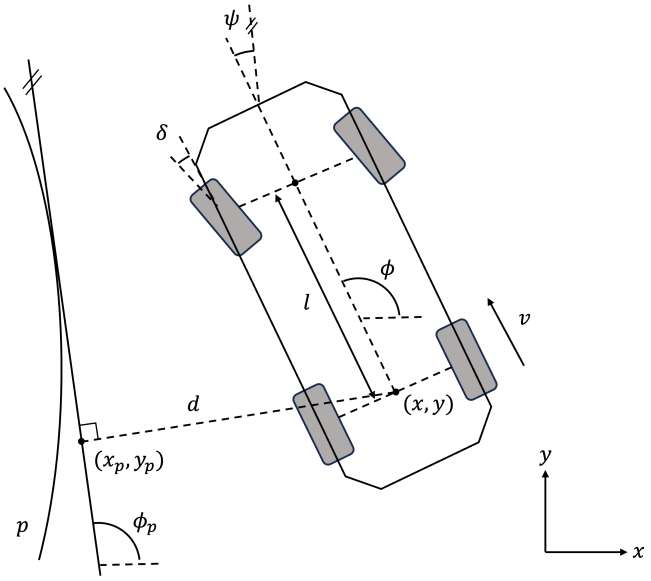

Fig. 1. Schematic of autonomous vehicle as a car-like vehicle model.

The vehicle's kinematics governing its motion can be expressed as follows:

$$\dot{\mathbf{x}}(t) = \begin{bmatrix} \dot{x}(t) \\ \dot{y}(t) \\ \dot{\phi}(t) \end{bmatrix} = \begin{bmatrix} v(t)\cos\phi(t) \\ v(t)\sin\phi(t) \\ \frac{v(t)}{l}\tan\delta(t) \end{bmatrix}. \tag{1}$$

Here, $v(t)$ and $\delta(t)$ represent the traction velocity of the rear wheels and the steering angle of the front wheels, respectively, serving as control inputs for the autonomous system.

As illustrated in Fig. 1, the path following schematic prioritizes minimizing the distance and orientation of the vehicle concerning the path p. The variable $d(t)$ indicates the closest distance between the vehicle's rear axle $(x(t), y(t))$ and the path (x_p, y_p), while $\psi(t)$ signifies the difference between the vehicle's orientation $\phi(t)$ and the path's orientation ϕ_p. Therefore, the distance and orientation of the vehicle concerning the path can be described using the following equations:

$$\begin{bmatrix} d(t) \\ \psi(t) \end{bmatrix} = \begin{bmatrix} ((x(t) - x_p^2 + (y(t) - y_p)^2)^{\frac{1}{2}} \\ \phi(t) - \phi_p \end{bmatrix}. \tag{2}$$

Assuming that the path configurations remain constant over a short time frame, the path following dynamics of the car-like vehicle can be defined as follows:

$$\begin{bmatrix} \dot{d}(t) \\ \dot{\psi}(t) \end{bmatrix} = \begin{bmatrix} v(t)\sin\phi(t) \\ \frac{v(t)}{l}\tan\delta(t) \end{bmatrix}. \tag{3}$$

This model forms the foundation for our investigation into sensor attacks and their impact on autonomous system.

B. State Space Formulation

The car-like vehicle kinematics model in the discrete-time model is represented as follows:

$$x_{k+1} = x_k + (\Delta t) v_k \cos\phi_k \tag{4}$$
$$y_{k+1} = y_k + (\Delta t) v_k \sin\phi_k \tag{5}$$
$$\phi_{k+1} = \phi_k + (\Delta t)\frac{v_k}{l}\tan\delta_k. \tag{6}$$

Then, the discrete-time state-space system (4)-(6) with sensor attack can be transformed into the following generic nonlinear state space model:

$$\mathbf{x}_{k+1} = \mathbf{A}\mathbf{x}_k + \mathbf{f}(\mathbf{x}_k, \mathbf{u}_k) \tag{7}$$
$$\mathbf{y}_k = \mathbf{C}\mathbf{x}_k + \mathbf{\Phi}\theta_k. \tag{8}$$

In this model, the state space equations consist of the state vector $\mathbf{x}_k \in \mathbb{R}^n$, the linear state transition matrix $\mathbf{A} \in \mathbb{R}^{n\times n}$, the nonlinear function $\mathbf{f} : \mathbb{R}^n \times \mathbb{R}^l \to \mathbb{R}^n$ with $\mathbf{u}_k = \begin{bmatrix} v_k & \delta_k \end{bmatrix}^\intercal$ denotes the control input vector, the measurement matrix $\mathbf{C} \in \mathbb{R}^{m\times n}$, the sensor attack profile matrix $\mathbf{\Phi} \in \mathbb{R}^{m\times q}$, the output vector as $\mathbf{y}_k \in \mathbb{R}^m$, and the sequence of sensor attack magnitudes as $\theta_k \in \mathbb{R}^q$.

In the absence of anomalies occurring from sensor malfunctions, any deviations are likely attributed to the attacks. To facilitate the estimation of these attacks via a nonlinear observer, we introduce a new state variable $\mathbf{w}_k \in \mathbb{R}^m$ which serves as a filtered version of the measurement equation (8), satisfying [21]:

$$\mathbf{w}_{k+1} = \mathbf{w}_k - \mathbf{A_{ft}}\mathbf{w}_k + \mathbf{A_{ft}}\mathbf{C}\mathbf{x}_k + \mathbf{A_{ft}}\mathbf{\Phi}\theta_k. \tag{9}$$

Here, $\mathbf{A_{ft}} = (\Delta t)\mathbf{A_f}$ with $-\mathbf{A_f} \in \mathbb{R}^{m\times m}$ represents a Hurwitz matrix. With this new state variable, we construct an augmented state vector:

$$\mathbf{z}_k = \begin{bmatrix} \mathbf{x}_k \\ \mathbf{w}_k \end{bmatrix} \in \mathbb{R}^p. \tag{10}$$

In this context, $p = m + n$ signifies the length of the augmented state vector. Consequently, the augmented discrete-time state-space model of the car-like vehicle system is as follows:

$$\mathbf{z}_{k+1} = \mathbf{A_a}\mathbf{z}_k + \mathbf{f_a}_k + \mathbf{\Phi_a}\theta_k \quad (11)$$

$$\mathbf{h}_k = \mathbf{C_a}\mathbf{z}_k \quad (12)$$

where

$$\mathbf{A_a} = \begin{bmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{A_{ft}C} & \mathbf{I}_m - \mathbf{A_{ft}} \end{bmatrix}, \mathbf{f_a}_k = \begin{bmatrix} \mathbf{f}(\mathbf{z}_k, \mathbf{u}_k) \\ \mathbf{0} \end{bmatrix},$$
$$\mathbf{\Phi_a} = \begin{bmatrix} \mathbf{0} \\ \mathbf{A_{ft}\Phi} \end{bmatrix}, \mathbf{C_a} = [\mathbf{0} \quad \mathbf{I}_m].$$

This augmented state-space model, as depicted in (11) and (12), serves as the foundation for the design of the nonlinear observer, allowing us to estimate the state variables and the magnitudes of sensor attacks.

III. DESIGNS

The primary objective of the control design is to achieve stability in the path following dynamics described in (3) at the origin, ensuring that the vehicle closely follows the desired path. The control inputs required to attain this goal are the traction velocity (v) and the steering angle (δ). Simultaneously, the objective of the nonlinear observer design is to detect and estimate sensor attacks effectively. By doing so, the controller can operate as intended, mitigating the impact of sensor attacks on the autonomous system's behavior.

To facilitate the design processes, several key assumptions are made:

Assumption 1. *The model assumes that there are no instances of slipping or skidding during the vehicle's motion, and it disregards sensor faults resulting from internal or external conditions.*

Assumption 2. *The control design exclusively considers forward motion, ensuring that $v > 0$. The physical limitations of the steering angle (δ) are bounded by $|\delta| \leq \frac{\pi}{5}$.*

Assumption 3. *The nonlinear function $\mathbf{f}$ adheres to one-sided Lipschitz and quadratic inner-boundedness conditions. In this context, for given values $\epsilon_1, \epsilon_2 > 0$, and parameters $\rho, \beta, \eta \in \mathbb{R}$, the following relationship holds ([22], [23]):*

$$\epsilon_1 \begin{bmatrix} \breve{\mathbf{z}}_k \\ \Delta\mathbf{f}_k \end{bmatrix}^\intercal \begin{bmatrix} \rho\mathbf{I}_p & -\frac{\mathbf{I}_p}{2} \\ -\frac{\mathbf{I}_p}{2} & \mathbf{0} \end{bmatrix} \begin{bmatrix} \breve{\mathbf{z}}_k \\ \Delta\mathbf{f}_k \end{bmatrix} \geq 0 \quad (13)$$

$$\epsilon_2 \begin{bmatrix} \breve{\mathbf{z}}_k \\ \Delta\mathbf{f}_k \end{bmatrix}^\intercal \begin{bmatrix} \beta\mathbf{I}_p & \frac{\eta\mathbf{I}_p}{2} \\ \frac{\eta\mathbf{I}_p}{2} & -\mathbf{I}_p \end{bmatrix} \begin{bmatrix} \breve{\mathbf{z}}_k \\ \Delta\mathbf{f}_k \end{bmatrix} \geq 0. \quad (14)$$

Here, $\breve{\mathbf{z}}_k = \mathbf{z}_k - \bar{\mathbf{z}}_k$ while $\Delta\mathbf{f}_k = \mathbf{f_a}_k - \bar{\mathbf{f}}_{\mathbf{a}k}$.

Remark 1. *The assumption presented in Assumption 3 is less stringent compared to the simple requirement that the function $\mathbf{f}$ be Lipschitz, as discussed in [24].*

These assumptions are essential in shaping our design approach for achieving stable path following dynamics and effective sensor attacks detection and estimation.

A. Path Following Control Design

The car-like vehicle system requires two essential control inputs: the traction velocity and the steering angle. Regarding the traction velocity, its design must be linked with the vehicle's position relative to the desired path (2) to ensure that the vehicle effectively follows the intended trajectory. The velocity is determined by the equation:

$$v(t) = \frac{v_{max}}{1 + k_d|d(t)| + k_\psi|\psi(t)|} > 0. \quad (15)$$

Here, v_{max} represents the maximum allowable traction velocity and $k_d, k_\psi > 0$. The positive velocity represents the forward movement of the vehicle. The relationship between velocity and the vehicle's position or orientation relative to the path is inversely proportional. When there is a substantial error in position or orientation concerning the path, the velocity is intentionally reduced to allow for the necessary adjustments in the vehicle's configuration.

Conversely, the control design for the steering angle focuses on stabilizing the path following dynamics described in (3) at the origin.

Theorem 1. *Consider the path following dynamics of a car-like vehicle system as described in* (3)*, with traction velocity in* (15)*. If Assumptions 1 and 2 are met, then the chosen steering angle:*

$$\delta(t) = -\arctan\left(\frac{l}{v}\left(k_\psi\psi(t) + v(t)d(t)\operatorname{sinc}\psi(t)\right)\right) \quad (16)$$

will make the equilibrium points $(d(t), \psi(t)) = \mathbf{0}$ asymptotically stable.

Proof. We choose a candidate Lyapunov function as follows:

$$V(d(t), \psi(t)) = \frac{1}{2}d(t)^2 + \frac{1}{2}\psi(t)^2. \quad (17)$$

The time derivative of V is:

$$\begin{aligned} \dot{V}(d(t), \psi(t)) &= d(t)\dot{d}(t) + \psi(t)\dot{\psi}(t) \\ &= d(t)v(t)\sin\phi(t) + \psi(t)\frac{v(t)}{l}\tan\delta(t) \end{aligned} \quad (18)$$

with δ defined in (16), the derivative becomes:

$$\dot{V}(d(t), \psi(t)) = -k_\psi\psi(t)^2 \leq 0. \quad (19)$$

According to Barbalat's lemma, since $\dot{V} \leq 0$ and is uniformly continuous, the value of $\dot{V} \to 0$ as $t \to \infty$, implying that only $\psi(t) \to 0$ fulfills the condition. Substituting (16) into (3) results in:

$$\begin{bmatrix} \dot{d}(t) \\ \dot{\psi}(t) \end{bmatrix} = \begin{bmatrix} v(t)\sin\psi(t) \\ -(k_\psi\psi(t) + v(t)d(t)\operatorname{sinc}\psi(t)) \end{bmatrix}. \quad (20)$$

Here, $\psi(t) \equiv 0$ implies $\dot{\psi}(t) \equiv 0$, and from the second row of (20), we deduce that $d = 0$ as $\lim_{\psi(t)\to 0}\operatorname{sinc}\psi(t) = 1$. Therefore, by employing Lasalle's invariance principle, we prove that the equilibrium points $(d(t), \psi(t)) = \mathbf{0}$ are asymptotically stable. ■

B. Observer Design

The primary objectives of the observer design is to estimate the state variables and the magnitudes of sensor attacks in a nonlinear system like the car-like vehicle. Referring to (11), the nonlinear observer can be designed as follows:

$$\bar{\mathbf{z}}_{k+1} = \mathbf{A_a}\bar{\mathbf{z}}_k + \bar{\mathbf{f}}_{\mathbf{a}k} + \mathbf{\Phi_a}\bar{\theta}_k - \mathbf{K}^{-1}\mathbf{L}^\intercal\breve{\mathbf{y}}_k \quad (21)$$

$$\bar{\theta}_{k+1} = \bar{\theta}_k + \mathbf{\Phi}_a^\intercal\mathbf{\Xi}(\breve{\mathbf{z}}_{k+1} - \mathbf{G}\breve{\mathbf{z}}_k - \Delta\mathbf{f}_k). \quad (22)$$

Here, $\breve{\mathbf{y}}_k = \mathbf{y}_k - \mathbf{C_a}\bar{\mathbf{z}}_k$, while $\bar{\mathbf{z}}_k$ and $\bar{\theta}_k$ denote the states and attack estimations and $\mathbf{K}$ and $\mathbf{L}$ represent the state observer gains. Both estimation gains are determined as follows:

$$\mathbf{G} = \mathbf{A_a} - \mathbf{K}^{-1}\mathbf{L}^\intercal\mathbf{C_a} \quad (23)$$

$$\mathbf{\Xi} = 2(\mathbf{\Phi_a}\mathbf{\Phi_a}^\intercal + \mathbf{Q})^{-1}. \quad (24)$$

In (24), $\mathbf{Q} = \mathbf{Q}^\intercal > 0 \in \mathbb{R}^{p\times p}$ acts as a tuning parameter for the attack estimations. It's worth noting that q and Q respectively stand for the smallest and largest eigenvalues of the matrix $\mathbf{Q}$. Similarly, for $\mathbf{K}$, its largest eigenvalue is represented by K, and for $\mathbf{\Phi}_a$, its largest eigenvalue is denoted as Φ.

To find the gains $\mathbf{K}$ and $\mathbf{L}$, we establish an error dynamics for the state and attack estimations using the nonlinear observer, as follows:

$$\breve{\mathbf{z}}_{k+1} = \mathbf{G}\breve{\mathbf{z}}_k + \Delta\mathbf{f}_k + \mathbf{\Phi_a}\bar{\theta}_k \quad (25)$$

$$\breve{\theta}_{k+1} = \breve{\theta}_k - \mathbf{\Phi_a}^\intercal\mathbf{\Xi}\mathbf{\Phi_a}\breve{\theta}_k. \quad (26)$$

Here, $\breve{\theta}_k = \theta_k - \bar{\theta}_k$.

Theorem 2. *Consider the error dynamics for state and attack estimations in* (25) *and* (26) *of the nonlinear observer given in* (21) *and* (22)*, provided that Assumption 3 is upheld. If there exist observer gains* $\mathbf{K} = \mathbf{K}^\intercal > 0 \in \mathbb{R}^{p\times p}$ *and* $\mathbf{L} \in \mathbb{R}^{m\times p}$ *that satisfy the following linear matrix inequalities (LMI):*

$$\begin{bmatrix} -\mathbf{K} + c_1\mathbf{I}_p & \mathbf{P}^\intercal + c_2\mathbf{I}_p & \mathbf{P}^\intercal \\ \mathbf{P} + c_3\mathbf{I}_p & \mathbf{K} + c_4\mathbf{I}_p & \mathbf{0} \\ \mathbf{P} & \mathbf{0} & -\mathbf{K} \end{bmatrix} \prec 0 \quad (27)$$

where $\mathbf{P} = \mathbf{K}\mathbf{A_a} - \mathbf{L}^\intercal\mathbf{C_a}$*,* $c_1 = \nu + \epsilon_1\rho + \epsilon_2\beta$*,* $c_2 = c_3 = \frac{\eta\epsilon_2 - \epsilon_1}{2}$*, and* $c_4 = -\epsilon_2$ *with* $\nu > 0$*. Then, the equilibrium points* $(\breve{\mathbf{z}}_k, \breve{\theta}_k) = \mathbf{0}$ *are globally uniformly asymptotically stable.*

Proof. Let V_k be a candidate Lyapunov function:

$$V_k = \breve{\mathbf{z}}_k^\intercal\mathbf{K}\breve{\mathbf{z}}_k + \alpha\breve{\theta}_k^\intercal\breve{\theta}_k \quad (28)$$

where $\alpha > 0$. Let ΔV_k be defined as $\Delta V_k = V_{k+1} - V_k$. Consequently, we have:

$$\Delta V_k = \breve{\mathbf{z}}_{k+1}^\intercal\mathbf{K}\breve{\mathbf{z}}_{k+1} - \breve{\mathbf{z}}_k^\intercal\mathbf{K}\breve{\mathbf{z}}_k + \alpha\breve{\theta}_{k+1}^\intercal\breve{\theta}_{k+1} - \alpha\breve{\theta}_k^\intercal\breve{\theta}_k. \quad (29)$$

By substituting (25) and (26) into (29) and utilizing the relationship $||\Delta\mathbf{f}_k|| \le c||\breve{\mathbf{z}}_k||$ with a sufficiently large constant $c > 0$, we obtain an inequality of:

$$\begin{aligned}\Delta V_k \le\ & \breve{\mathbf{z}}_k^\intercal(\mathbf{G}^\intercal\mathbf{K}\mathbf{G} - \mathbf{K})\breve{\mathbf{z}}_k + \Delta\mathbf{f}_k^\intercal\mathbf{K}\Delta\mathbf{f}_k \\ & + 2\breve{\mathbf{z}}_k^\intercal\mathbf{G}^\intercal\mathbf{K}\Delta\mathbf{f}_k + 2\breve{\theta}_k^\intercal\mathbf{\Phi}_a^\intercal\mathbf{K}(\mathbf{G} + c\mathbf{I}_p)\breve{\mathbf{z}}_k \\ & - \breve{\theta}_k^\intercal\mathbf{\Phi}_a^\intercal(\alpha\mathbf{\Xi}\mathbf{Q}\mathbf{\Xi} - \mathbf{K})\mathbf{\Phi}_a\breve{\theta}_k.\end{aligned} \quad (30)$$

By referring to (24) and the eigenvalues of the matrices, the last two terms of the right-hand side of (30) are bounded, resulting in (30) becomes:

$$\begin{aligned}\Delta V_k \le\ & \breve{\mathbf{z}}_k^\intercal(\mathbf{G}^\intercal\mathbf{K}\mathbf{G} - \mathbf{K})\breve{\mathbf{z}}_k + \Delta\mathbf{f}_k^\intercal\mathbf{K}\Delta\mathbf{f}_k \\ & + 2\breve{\mathbf{z}}_k^\intercal\mathbf{G}^\intercal\mathbf{K}\Delta\mathbf{f}_k + \nu\breve{\mathbf{z}}_k^\intercal\breve{\mathbf{z}}_k \\ & - \left(\frac{4\alpha q}{(\Phi^2 + Q)^2} - K - \frac{K^2\mu^2}{\nu}\right)||\mathbf{\Phi}_a\breve{\theta}_k||^2\end{aligned} \quad (31)$$

with $\mu = ||\mathbf{G} + c\mathbf{I}_p||_2$. If we set α as:

$$\alpha > \frac{(\Phi^2 + Q)^2}{4q}\left(K + \frac{K^2\mu^2}{\nu}\right), \quad (32)$$

the simplified version of (31) is:

$$\begin{aligned}\Delta V_k \le\ & \breve{\mathbf{z}}_k^\intercal(\mathbf{G}^\intercal\mathbf{K}\mathbf{G} - \mathbf{K} + \nu\mathbf{I}_p)\breve{\mathbf{z}}_k + \Delta\mathbf{f}_k^\intercal\mathbf{K}\Delta\mathbf{f}_k \\ & + 2\breve{\mathbf{z}}_k^\intercal\mathbf{G}^\intercal\mathbf{K}\Delta\mathbf{f}_k.\end{aligned} \quad (33)$$

Defining $\mathbf{r}_k = \begin{bmatrix}\breve{\mathbf{z}}_k & \Delta\mathbf{f}_k\end{bmatrix}^\intercal$, this can be rewritten as follows:

$$\Delta V_k \le \mathbf{r}_k^\intercal\begin{bmatrix}\mathbf{G}^\intercal\mathbf{K}\mathbf{G} - \mathbf{K} + \nu\mathbf{I}_p & \mathbf{G}^\intercal\mathbf{K} \\ \mathbf{K}\mathbf{G} & \mathbf{K}\end{bmatrix}\mathbf{r}_k \quad (34)$$

By incorporating the one-sided Lipschitz (13) and quadratic inner-boundedness (14) conditions into the right-hand side of (34), will result in an inequality of [25]:

$$\Delta V_k \le \mathbf{r}_k^\intercal\begin{bmatrix}\mathbf{G}^\intercal\mathbf{K}\mathbf{G} - \mathbf{K} + c_1\mathbf{I}_p & \mathbf{G}^\intercal\mathbf{K} + c_2\mathbf{I}_p \\ \mathbf{K}\mathbf{G} + c_3\mathbf{I}_p & \mathbf{K} + c_4\mathbf{I}_p\end{bmatrix}\mathbf{r}_k. \quad (35)$$

We obtain $\Delta V_k \le 0$, if the matrix on the right-hand side of (35) satisfies:

$$\begin{bmatrix}\mathbf{G}^\intercal\mathbf{K}\mathbf{G} - \mathbf{K} + c_1\mathbf{I}_p & \mathbf{G}^\intercal\mathbf{K} + c_2\mathbf{I}_p \\ \mathbf{K}\mathbf{G} + c_3\mathbf{I}_p & \mathbf{K} + c_4\mathbf{I}_p\end{bmatrix} < 0. \quad (36)$$

Here, $\mathbf{G}$ is derived from (23). Applying the Schur complement to (36) with respect to $\mathbf{G}^\intercal\mathbf{K}\mathbf{G} - \mathbf{K} + c_1\mathbf{I}_p < 0$, we arrive at (27). Hence, by utilizing Lasalle's invariance principle, we establish that the equilibrium points $(\breve{\mathbf{z}}_k, \breve{\theta}_k) = \mathbf{0}$ are proven to be globally uniformly asymptotically stable. ■

IV. NUMERICAL SIMULATIONS

We conduct simulations of path following control of an autonomous vehicle to validate the effectiveness of the proposed nonlinear observer design, with the designed traction velocity and steering angle serving as the control inputs to maneuver the car-like vehicle along the designated path while sensor attacks are present. The measurement matrix is set to:

$$\mathbf{C} = \begin{bmatrix}1 & 0 & 0 \\ 0 & 1 & 0\end{bmatrix}, \quad (37)$$

signifying that the attacks target the vehicle's localization system in Cartesian coordinates. This implies that the magnitudes of sensor attacks $\theta_k \in \mathbb{R}^2$, correspond to the given attack profile matrix $\mathbf{\Phi} = \mathbf{I}_2$.

To provide a clear demonstration of our approach in addressing sensor attacks on autonomous systems, the path following simulations encompass two scenarios: one with state feedback from spoofed measurements and the other with state feedback from the estimated state by the nonlinear observer. Both scenarios employ the designed control inputs

v and δ as described in (15) and (16). For these simulations, certain control parameters need to be determined, which are:

$$l = 3 \text{ m}, v_{max} = 2 \text{ m/s}, k_d = k_\psi = 2. \tag{38}$$

The magnitudes of the attacks are modeled to simulate the real-world scenario of sensor spoofing. This allows us to observe how the path following dynamics behave when exposed to sensor attacks.

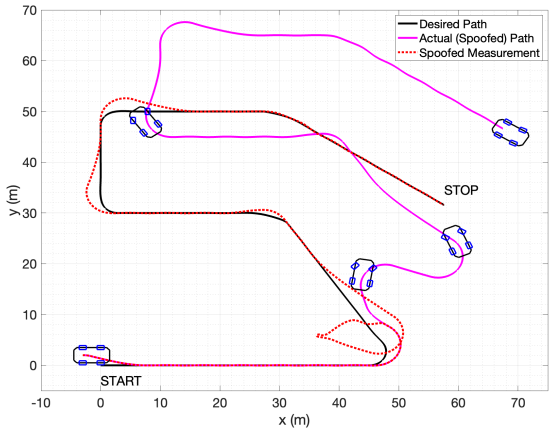

Fig. 2. Path following simulation with spoofed measurements as feedback signals.

In Fig. 2, the results of the path following simulations for the first scenario are presented. The red striped line represents spoofed measurements, while the solid magenta line indicates the actual trajectory of the vehicle's motion influenced by the spoofed measurements. The spoofed measurement attacks commence after 70 s of simulation, specifically at coordinates $(47.56, 8.18)$ m in the Cartesian plane. It's evident that the vehicle initially follows the designated path reasonably well until the attacks are initiated. However, the system is unable to mitigate the attack, resulting in a significant deviation from the intended path. The spoofed measurements mislead the system by providing incorrect measurements disguised as correct ones.

In the second scenario, the nonlinear observer is employed for secure state estimation, offering state feedback in the form of an estimation to the control system. However, prior to implementation, the determination of observer gains is required, a process accomplished through a heuristic method. The parameters of the LMI are set as follows $\epsilon_1 = 1$, $\epsilon_2 = 100$, $\nu = 0.01$, $\rho = -10$, and $\beta = 0.01$. Additionally, the observer gains are chosen as $\mathbf{Q} = 0.1\mathbf{I}_5$ and:

$$\mathbf{K} = 10\mathbf{I}_5, \tag{39}$$

$$\mathbf{L} = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{40}$$

that satisfy the LMI defined in (27).

The path following using the state estimation provided by the nonlinear observer as feedback for the control system is depicted in Fig. 3. The solid blue line illustrates the vehicle's motion trajectories along the path while sensor

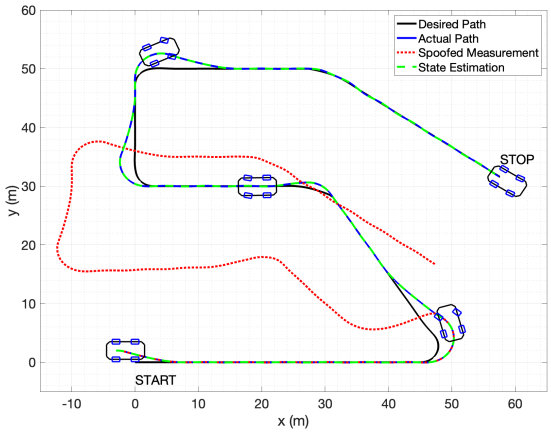

Fig. 3. Path following simulation with estimated state by the nonlinear observer as feedback signals.

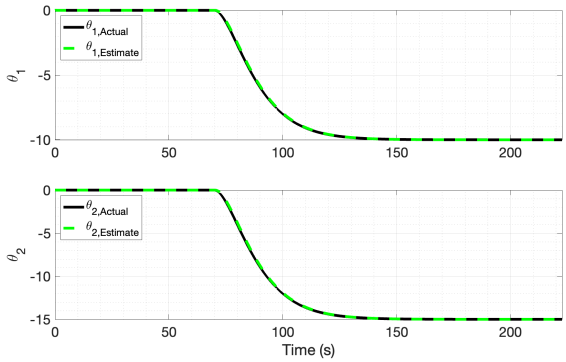

Fig. 4. Actual magnitude of the sensor attacks and their estimation values by the nonlinear observer.

attacks are present. Spoofing initiates at the same time and place as in the first scenario, but there are no indications of the vehicle deviating from the path. Some slight overshoots occur, influenced by factors such as the vehicle's length, the sharp curvature of the path, and the actuator's saturation.

To quantitatively evaluate the performance of the designed control and observer, we calculated the root mean squared errors (RMSEs) for the position and orientation of the vehicle relative to the designated path (including the initial conditions). These errors are found to be 1.43 m and 0.23 rad, respectively. The estimation of sensor attack magnitudes is presented in Fig. 4 with the blue striped line indicating the estimated values. As observed, the estimation converges to the actual values with a high level of accuracy. The RMSEs for both attacks are 0.04 m for the horizontal position (x-axis) and 0.06 m for the vertical position (y-axis). The MATLAB simulations were executed with an average loop time of 0.1 ms and a total simulation duration of 345.7 ms, highlighting the viability of practical implementation due to its rapid computational performance, as well as its light computational load.

Overall, the proposed nonlinear observer design accurately estimates the states and the attacks, allowing the proposed

controller to maneuver the vehicle to closely follow the intended path. The control is derived using the Lyapunov approach, making it robust and sufficiently accurate. And the guaranteed stability and accuracy of the proposed nonlinear observers with minimal computational efforts render it suitable for implementation in real-world applications, where it can effectively mitigate attacks on the sensors and prevent critical situations in autonomous systems.

V. CONCLUSIONS

In this study, we investigated sensor attacks on autonomous systems, with a particular focus on attacks targeting the localization system of autonomous vehicles during path following control. Our proposed control algorithm has successfully demonstrated its ability to ensure the stability of path following dynamics under the presence of sensor attacks, using the state feedback received from the proposed nonlinear observer. By formulating sensor attacks into a filtered form, our observer can estimate the magnitudes of these attacks as states of the augmented system. The numerical simulations have showcased the robustness and precision of the proposed observer in estimating both the states and the magnitudes of sensor attacks, thereby enabling the control algorithm to perform as intended even in the presence of such attacks. Further investigations may explore the development of control and observer designs customized for a variety of system types that could be vulnerable to sensor attacks. Additionally, we can delve into strategies for concurrently mitigating attacks on both the actuators and sensors in autonomous systems. Furthermore, evaluating the performance of our proposed observer in the presence of noise or system uncertainties presents promising avenues for future research.

REFERENCES

[1] S. Shah, I. Logiotatopouloh, and S. Menon, "Industry 4.0 and autonomous transportation: the impacts on supply chain management," *Journal of Intelligent Transportation Systems*, vol. 4, pp. 45–50, 08 2019.

[2] E. E. Ambarita, A. Karlsen, O. Osen, and A. Hasan, "Towards fully autonomous floating offshore wind farm operation & maintenance," *Energy Reports*, vol. 9, pp. 103–108, 2023.

[3] Y. J. Qu, X. G. Ming, Z. Liu, X. Zhang, and Z. T. Hou, "Smart manufacturing systems: state of the art and future trends," *The International Journal of Advanced Manufacturing Technology*, pp. 1–18, 2019.

[4] E. Coiera, "The fate of medicine in the time of ai." *Lancet*, vol. 392, pp. 2331–2332, 12/2018 2018.

[5] M. Saidani, E. Pan, H. Kim, A. Greenlee, J. Wattonville, B. Yannou, Y. Leroy, and F. Cluzel, "Assessing the environmental and economic sustainability of autonomous systems: A case study in the agricultural industry," *Procedia CIRP*, vol. 90, pp. 209–214, 2020.

[6] I. Kuncara, A. Widyotriatmo, and A. Hasan, "On detection and size estimation of cyber-attacks against autonomous systems," in *IECON 2023-49th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2023, pp. 1–6.

[7] B. Zou, P. Choobchian, and J. Rozenberg, "Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies," *Journal of Transportation Security*, vol. 14, pp. 137–155, 2021.

[8] E. E. Ambarita, I. Kuncara, A. Widyotriatmo, A. Karlsen, F. Scibilia, and A. Hasan, "On cyber-attacks against wind farms," in *IECON 2023-49th Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2023, pp. 1–6.

[9] Y. Wang, N. Bian, L. Zhang, Y. Huang, and H. Chen, "Resilient path-following control of autonomous vehicles subject to intermittent denial-of-service attacks," *IET Intelligent Transport Systems*, vol. 15, no. 12, pp. 1508–1521, 2021.

[10] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, and M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," *Ad Hoc Networks*, vol. 111, p. 102324, 2021.

[11] F. Alrefaei, A. Alzahrani, H. Song, and S. Alrefaei, "A survey on the jamming and spoofing attacks on the unmanned aerial vehicle networks," in *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 2022, pp. 1–7.

[12] J. Shin, Y. Baek, Y. Eun, and S. H. Son, "Intelligent sensor attack detection and identification for automotive cyber-physical systems," in *2017 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2017, pp. 1–8.

[13] H. Cam, "Cyber resilience using autonomous agents and reinforcement learning," in *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications II*, ser. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, T. Pham, L. Solomon, and K. Rainey, Eds., vol. 11413, Apr. 2020, p. 114130R.

[14] F. Akowuah and F. Kong, "Real-time adaptive sensor attack detection in autonomous cyber-physical systems," in *2021 IEEE 27th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, 2021, pp. 237–250.

[15] S. Dasgupta, M. Rahman, M. Islam, and M. Chowdhury, "A sensor fusion-based gnss spoofing attack detection framework for autonomous vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 12, pp. 23 559–23 572, 2022.

[16] Y. Shoukry, P. Nuzzo, A. Puggelli, A. L. Sangiovanni-Vincentelli, S. A. Seshia, and P. Tabuada, "Secure state estimation for cyber-physical systems under sensor attacks: A satisfiability modulo theory approach," *IEEE Transactions on Automatic Control*, vol. 62, no. 10, pp. 4917–4932, 2017.

[17] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, "Detection and isolation of sensor attacks for autonomous vehicles: Framework, algorithms, and validation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 23, no. 7, pp. 8247–8259, 2022.

[18] I. Kuncara, A. Widyotriatmo, and A. Hasan, "Observer design for autonomous systems under sensor attacks," in *2023 62nd IEEE Conference on Decision and Control (CDC)*. IEEE, 2023, pp. 2815–2820.

[19] R. G. Dutta, X. Guo, T. Zhang, K. Kwiat, C. Kamhoua, L. Njilla, and Y. Jin, "Estimation of safe sensor measurements of autonomous system under attack," in *2017 54th ACM/EDAC/IEEE Design Automation Conference (DAC)*, 2017, pp. 1–6.

[20] L. Ma, Z. Wang, Q.-L. Han, and H.-K. Lam, "Variance-constrained distributed filtering for time-varying systems with multiplicative noises and deception attacks over sensor networks," *IEEE Sensors Journal*, vol. 17, no. 7, pp. 2279–2288, 2017.

[21] C. Edwards and C. P. Tan, "A comparison of sliding mode and unknown input observers for fault reconstruction," *European Journal of Control*, vol. 12, no. 3, pp. 245–260, 2006.

[22] A. Hasan, M. Tahavori, and H. S. Midtiby, "Model-based fault diagnosis algorithms for robotic systems," *IEEE Access*, vol. 11, pp. 2250–2258, 2023.

[23] A. Hasan, "Observer-based fault diagnosis for autonomous systems," *International Journal of Robust and Nonlinear Control*, 2024.

[24] M. Abbaszadeh and H. Marquez, "Nonlinear observer design for one-sided lipschitz systems," in *Proceedings of the 2010 American Control Conference, ACC 2010*, vol. 6, 08 2010, pp. 5284 – 5289.

[25] A. Hasan, "exogenous kalman filter for state estimation in autonomous ball balancing robots," in *2020 IEEE/ASME International Conference on Advanced Intelligent Mechatronics (AIM)*, 2020, pp. 1522–1527.