2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Observer Design for Autonomous Systems under Sensor Attacks

Ivan Kuncara[1], Augie Widyotriatmo[1], and Agus Hasan[2]

Abstract— **As autonomous systems become more widespread, they are increasingly vulnerable to sensor attacks. In this paper, we propose a novel observer designed to estimate the magnitude of sensor attacks on autonomous systems. Our proposed observer is a discrete-time observer that can be used for joint estimation of both state and parameters. The key idea behind our proposed observer is to filter the measurement and augment the measurement equation into the state space model. Our proposed observer has several advantages over existing methods. First, the filtering of the measurement and augmentation of the measurement equation enable the observer to account for the impact of sensor attacks on both the state and the parameters of the system. Second, the joint estimation of state and parameters enables the observer to adapt to changing conditions and maintain accurate estimates over time. We demonstrate the effectiveness of our proposed observer through numerical simulations. Our results show that the observer is capable of accurately estimating the magnitude of sensor attacks on autonomous systems.**

I. INTRODUCTION

Sensor attacks on autonomous systems are a critical issue because they can have severe consequences, including safety risks, economic damage, and loss of privacy [1]. Autonomous systems such as self-driving cars, drones, and industrial robots rely heavily on sensors to perceive and interact with their environment. Therefore, if the sensors are compromised, the autonomous system may receive false or misleading information, which can lead to disastrous consequences. For example, if a self-driving car's LiDAR sensor is attacked and the sensor output is manipulated to misrepresent the distance and location of objects in the car's path, the car could potentially collide with other vehicles or pedestrians [2]. Similarly, if a drone's GPS signal is hacked, the drone could fly off course and potentially cause damage or injury.

In addition to safety risks, sensor attacks can also result in economic damage. For instance, if an industrial robot's sensor is hacked, it may damage the products being manufactured, leading to a loss of revenue for the company. Moreover, sensor attacks can also compromise the privacy of individuals, as they can be used to collect sensitive information or track individuals without their knowledge or consent. Thus, it is critical to ensure that autonomous systems' sensors are secure and resilient to attacks [3]. This requires implementing robust security measures such as encryption, authentication, and intrusion detection to prevent malicious actors from exploiting vulnerabilities in the sensors. It also requires ongoing monitoring and testing of the sensors' performance to identify any potential vulnerabilities.

A. Literature Review

Sensor attacks against autonomous systems can be executed in various ways, depending on the type of attack and the system's specific vulnerabilities. The two most common sensor attacks are spoofing and jamming [4]. Sensor spoofing is a type of attack where an attacker deceives an autonomous system by impersonating a legitimate signal from a sensor. The attacker aims to manipulate the sensor's output by creating false sensor data that the autonomous system interprets as genuine. The attacker can use different methods to spoof the sensor's output, such as mimicking the sensor's signal by transmitting signals with the same frequency, modulation, and timing characteristics as the legitimate signal, replaying previously recorded signals, or creating entirely fake signals [5]. Sensor jamming is another type of attack where an attacker disrupts or blocks the signal between a sensor and an autonomous system. The attacker aims to disrupt the sensor's communication with the system by creating interference in the signal. The attacker can use various methods to jam the sensor's signal, such as transmitting noise in the same frequency range as the sensor's signal, which overwhelms and disrupts the legitimate signal, or using a more focused jamming technique, such as directional jamming, to target specific sensors or portions of the signal [6]. To prevent sensor spoofing and jamming, proper security measures such as using encryption and spread spectrum techniques must be implemented, which makes the signal harder to jam or spoof. Additionally, deploying multiple sensors and redundant communication channels can help mitigate the impact of sensor attacks by providing backup sources of data for the autonomous system. Other techniques, such as directional antennas, frequency agility, and power control, can also be used to detect and counteract spoofing and jamming.

In recent years, significant progress has been made in the area of sensor attack diagnosis using secure state estimation [7]. Secure state estimation is concerned with accurately estimating the state of a system while ensuring that the estimation process is not affected by malicious attacks [8]. This is particularly important for systems that rely on sensor measurements, as inaccurate measurements due to sensor attacks can lead to incorrect state estimates and potentially catastrophic consequences. Traditional state estimation techniques use sensor measurements to estimate the system's

*This work was supported by Institut Teknologi Bandung and Equinor.

[1]I. Kuncara and A. Widyotriatmo are with Instrumentation and Control Research Group, Faculty of Industrial Technology, Institut Teknologi Bandung, Bandung, Indonesia

[2]A. Hasan is with Department of ICT and Natural Sciences, Norwegian University of Science and Technology, 6009 Alesund, Norway and Department of Mathematics, Institute Technology Bandung, Bandung, Indonesia agus.hasan@ntnu.no

state, which can then be used to control the system or make decisions. However, if a sensor is compromised by an attacker, the measurements it provides may be inaccurate [9], [10]. Secure state estimation techniques aim to address this issue by detecting and mitigating the effects of sensor attacks on state estimation. One approach to secure state estimation is to develop state observers that can diagnose sensor faults or attacks by comparing the estimated state of the system with its actual state. Observers can be used to identify whether a sensor is malfunctioning or has been subjected to an attack by analyzing discrepancies between the estimated and actual system states. By using observers for sensor attack diagnosis, it is possible to detect and mitigate the effects of sensor attacks on state estimation, thereby ensuring the safety and security of the system [11].

In [12], a method for achieving secure state estimation using a Satisfiability Modulo Theory (SMT) approach is presented. The authors demonstrate that the problem of state estimation can be formulated as a satisfiability problem that includes logic and pseudo-Boolean constraints on Boolean variables, as well as convex constraints on real variables. Building on this work, [13] introduces an observer architecture based on SMT that is able to efficiently estimate the states of a discrete-time linear-time-invariant system in the presence of sensor attacks and measurement noise. The proposed algorithm is scalable and can be implemented for large systems, unlike many previously proposed algorithms that suffer from excessive memory and time requirements. Another approach for secure state estimation for sensor attacks was presented in [14] based on Kalman filter. The authors propose an alternative approach for achieving secure state estimation in the presence of sensor attacks based on the Kalman filter. The proposed method is designed to be computationally efficient, and is able to handle arbitrary and unbounded attacks by assuming that the set of attacked sensors can change over time. To evaluate the performance of their approach, the authors conduct numerical simulations and compare the results with those obtained using a standard Kalman filter. The simulation results demonstrate that the proposed secure estimator outperforms the standard Kalman filter, indicating the effectiveness of the approach.

B. Contribution of this Paper

The aforementioned references in sub-section A, presented approaches for achieving secure state estimation in the presence of sensor attacks. However, these methods did not address the issue of quantifying the magnitude of the attacks. In order to design effective controllers that can compensate for the attacks, it is necessary to have information about the severity of the attacks. This is the problem that we aim to address in our paper. Specifically, we propose a method for designing observers that can be used for secure state estimation while also accurately estimating the magnitude of sensor attacks. By incorporating this information into our design, we can improve the performance of control systems by allowing for more accurate compensation for the attacks. We demonstrate the effectiveness of our proposed observer through numerical simulations. These simulations illustrate how our approach can accurately estimate the magnitude of the sensor attacks and provide more reliable estimates of the system's state. This, in turn, can lead to improved control performance and better overall system stability.

C. Organization of this Paper

This paper is organized as follows. In Section II, we formulate the problem that we aim to solve. In Section III, we present the design of the observer. Specifically, we propose an observer based on a discrete-time exponential forgetting factor observer. The design and implementation of the observer is discussed in detail. In Section IV, we compare the performance of the observer and provide a thorough analysis of the results. Finally, in Section V, we conclude the paper by summarizing our findings and discussing possible directions for future research. We highlight the significance of our work in addressing the identified problem and discuss potential avenues for further exploration in this area.

II. PROBLEM FORMULATION

We consider autonomous systems that can be modelled into the following discrete-time state space system:

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}\mathbf{x}_k + \mathbf{f}(\mathbf{x}_k) + \mathbf{B}\mathbf{u}_k && (1)\\ \mathbf{y}_k &= \mathbf{C}\mathbf{x}_k + \mathbf{\Phi}\theta_k && (2) \end{aligned}$$

Here, $\mathbf{x}_k \in \mathbb{R}^n$ denotes the state variable, $\mathbf{u}_k \in \mathbb{R}^m$ is the control input, $\mathbf{y}_k \in \mathbb{R}^p$ is the output, and $\theta_k \in \mathbb{R}^q$ is the sensor attack signals. $\mathbf{f} : \mathbb{R}^n \to \mathbb{R}^n$ is the nonlinear function and is assumed to be continuously differentiable. The state matrix is denoted by $\mathbf{A} \in \mathbb{R}^{n\times n}$, the input matrix is denoted by $\mathbf{B} \in \mathbb{R}^{n\times m}$, the output matrix is denoted by $\mathbf{C} \in \mathbb{R}^{p\times n}$, and the matrix associated with the sensor attack is denoted by $\mathbf{\Phi} \in \mathbb{R}^{p\times q}$. We assume the sensor is in perfect working condition, and any anomalies observed are likely to be caused by cyber-attacks rather than an internal sensor fault. The idea of this paper is first to filter the measurement equation (2) into the following state equation [15]:

$$\mathbf{h}_{k+1} = \mathbf{A_f}\mathbf{h}_k - \mathbf{A_f}\mathbf{C}\mathbf{x}_k - \mathbf{A_f}\mathbf{\Phi}\theta_k \quad (3)$$

where $\mathbf{A_f} \in \mathbb{R}^{p\times p}$ is a stable matrix, i.e, $-\mathbf{A_f}$ is a Hurwitz matrix. Rearranging and augmenting (3) into (1), we have:

$$\begin{aligned} \mathbf{x}_{k+1} &= \mathbf{A}\mathbf{x}_k + \mathbf{f}(\mathbf{x}_k) + \mathbf{B}\mathbf{u}_k && (4)\\ \mathbf{h}_{k+1} &= -\mathbf{A_f}\mathbf{C}\mathbf{x}_k + \mathbf{A_f}\mathbf{h}_k - \mathbf{A_f}\mathbf{\Phi}\theta_k && (5) \end{aligned}$$

If we define the augmented state as:

$$\mathbf{z}_k = \begin{pmatrix} \mathbf{x}_k \\ \mathbf{h}_k \end{pmatrix} \quad (6)$$

then, we have:

$$\begin{aligned} \mathbf{z}_{k+1} &= \mathcal{A}\mathbf{z}_k + \mathcal{F}(\mathbf{z}_k) + \mathcal{B}\mathbf{u}_k + \mathbf{\Psi}\theta_k && (7)\\ \mathcal{Y}_k &= \mathcal{C}\mathbf{z}_k && (8) \end{aligned}$$

where

$$\mathcal{A} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ -\mathbf{A_f C} & \mathbf{A_f} \end{pmatrix}, \quad \mathcal{F}(\mathbf{z}_k) = \begin{pmatrix} \mathbf{f}(\mathbf{z}_k) \\ \mathbf{0} \end{pmatrix}, \mathcal{B} = \begin{pmatrix} \mathbf{B} \\ \mathbf{0} \end{pmatrix},$$
$$\mathcal{C} = \begin{pmatrix} \mathbf{0} & \mathbf{I} \end{pmatrix}, \quad \mathbf{\Psi} = \begin{pmatrix} \mathbf{0} \\ -\mathbf{A_f \Phi} \end{pmatrix}$$

The sensor attacks problem (1)-(2) is now translated into an adaptive observer design problem (7)-(8).

Remark 1: If $\mathbf{f}$ is zero or if all states can be measured, then we can approach this problem by defining an augmented state $\mathcal{Z}_k = \begin{pmatrix} \mathbf{z}_k & \theta_k \end{pmatrix}^\intercal$ with $\theta_{k+1} = \theta_k = \theta$. In this case, we have:

$$\mathcal{Z}_{k+1} = \bar{\mathcal{A}}\mathcal{Z}_k + \bar{\mathcal{B}}_k \tag{9}$$
$$\mathcal{Y}_k = \bar{\mathcal{C}}\mathcal{Z}_k \tag{10}$$

where

$$\bar{\mathcal{A}} = \begin{pmatrix} \mathcal{A} & \mathbf{\Psi} \\ \mathbf{0} & \mathbf{I} \end{pmatrix}, \ \bar{\mathcal{B}}_k = \begin{pmatrix} \mathcal{B}\mathbf{u}_k \\ \mathbf{0} \end{pmatrix}, \ \bar{\mathcal{C}} = \begin{pmatrix} \mathcal{C} & \mathbf{0} \end{pmatrix} \tag{11}$$

An observer for (9) can be designed using several methods, such as Kalman filter and particle filter. In [16], an observer for (9) is designed as follows:

$$\bar{\mathcal{Z}}_{k|k} = \bar{\mathcal{Z}}_{k|k-1} + \mathbf{K}_k \left(\mathcal{Y}_k - \bar{\mathcal{C}}\bar{\mathcal{Z}}_{k|k-1} \right) \tag{12}$$

where the observer gains $\mathbf{K}_k$ is calculated using the following formula:

$$\mathbf{K}_k = \mathbf{P}_{k|k-1}\bar{\mathcal{C}}^\intercal \left(\bar{\mathcal{C}}\mathbf{P}_{k|k-1}\bar{\mathcal{C}}^\intercal + \mathbf{R}_k \right)^{-1} \tag{13}$$

with the predictions update

$$\bar{\mathcal{Z}}_{k+1|k} = \bar{\mathcal{A}}\bar{\mathcal{Z}}_k + \bar{\mathcal{B}}_k \tag{14}$$
$$\mathbf{P}_{k+1|k} = \lambda^{-1}\bar{\mathcal{A}} \left(\mathbf{P}_{k|k-1} - \mathbf{P}_{k|k-1}\mathcal{C}^\intercal \left(\mathcal{C}\mathbf{P}_{k|k-1}\mathcal{C}^\intercal + \mathbf{R}_k \right)^{-1} \mathcal{C}\mathbf{P}_{k|k-1} \right) \bar{\mathcal{A}}^\intercal \tag{15}$$

where $\mathbf{P}_{k|k-1}$ and $\mathbf{R}_k$ are symmetric positive definite matrices, and $\lambda \in (0, 1)$. The dynamical extension approach has an important consequence that the observer's dynamics cannot be separated for each of the two quantities being estimated. However, it is not necessary to estimate constant parameters at the same rate as variables with non-trivial dynamics need to be tracked. As a result, there is an incentive to create an observer that differentiates between the two constituents of the extended state vector and allocates distinct estimation dynamics to each of them.

To simplify the problem, linearizing (7) at $\bar{\mathbf{z}}_{k+1}$, yields:

$$\mathbf{z}_{k+1} = \mathbf{F}_k\mathbf{z}_k + \mathbf{E}_k + \mathcal{B}\mathbf{u}_k + \mathbf{\Psi}\theta_k \tag{16}$$

where $\mathbf{F}_k$ and $\mathbf{E}_k$ are defined as:

$$\mathbf{F}_k = \mathcal{A} + \left. \frac{\partial \mathcal{F}(\mathbf{z}_k)}{\partial \mathbf{z}_k} \right|_{\bar{\mathbf{z}}_{k+1}} \tag{17}$$

$$\mathbf{E}_k = \mathcal{F}(\bar{\mathbf{z}}_{k+1}) - \left(\left. \frac{\partial \mathcal{F}(\mathbf{z}_k)}{\partial \mathbf{z}_k} \right|_{\bar{\mathbf{z}}_{k+1}} \right) \bar{\mathbf{z}}_{k+1} \tag{18}$$

The simplified sensor attacks problem (1)-(2) is now equivalent to an adaptive observer design problem for the following system:

$$\mathbf{z}_{k+1} = \mathbf{F}_k\mathbf{z}_k + \mathbf{E}_k + \mathcal{B}\mathbf{u}_k + \mathbf{\Psi}\theta_k \tag{19}$$
$$\mathcal{Y}_k = \mathcal{C}\mathbf{z}_k \tag{20}$$

To this end, we impose the following assumption:

Assumption 1: $\mathbf{F}_k$ is invertible for all k.

Assumption 2: The homogenous system $\mathbf{z}_{k+1} = \mathbf{F}_k\mathbf{z}_k$ with $\mathcal{Y}_k = \mathcal{C}\mathbf{z}_k$ is completely uniformly observable.

III. OBSERVER DESIGN

In Section II, we have demonstrated that the issue of sensor attacks can be reformulated as an adaptive observer design problem. Building on this, in this section, we present our proposed solution to the problem by designing an adaptive observer based on the discrete-time exponential forgetting factor observer, as outlined in [16]. The primary goal of our proposed observer design is to estimate the system state variables accurately, even in the presence of sensor attacks. However, it is essential to note that the observer is designed for a deterministic scenario, without considering the presence of noise. We base our design on the exponential forgetting factor observer, which is a commonly used technique for state estimation in systems with slowly varying dynamics. Our proposed observer incorporates an adaptive mechanism that continuously updates its parameters to adapt to changes in the system's dynamics. This adaptation allows the observer to maintain its accuracy and reliability even in the face of significant variations in the system's parameters. Through simulations, we demonstrate the effectiveness of our proposed observer design in mitigating the impact of sensor attacks and accurately estimating the system state variables.

A. Adaptive Observer Design

The adaptive observer is designed as follow:

$$\bar{\mathbf{z}}_{k|k} = \bar{\mathbf{z}}_{k|k-1} + \left(\mathbf{K}_k^{\mathbf{z}} + \mathbf{\Gamma}_{k|k}\mathbf{K}_k^{\theta} \right) \left(\mathcal{Y}_k - \mathcal{C}\bar{\mathbf{z}}_{k|k-1} \right) \tag{21}$$
$$\bar{\theta}_{k|k} = \bar{\theta}_{k|k-1} - \mathbf{K}_k^{\theta}(\mathcal{Y}_k - \mathcal{C}\bar{\mathbf{z}}_{k|k-1}) \tag{22}$$

where the observer gains $\mathbf{K}_k^{\mathbf{z}}$, $\mathbf{K}_k^{\theta}$, and $\mathbf{\Gamma}_{k|k}$ are calculated from the following formulas:

$$\mathbf{K}_k^{\mathbf{z}} = \mathbf{P}_{k|k-1}^{\mathbf{z}}\mathcal{C}^\intercal \left(\mathcal{C}\mathbf{P}_{k|k-1}^{\mathbf{z}}\mathcal{C}^\intercal + \mathbf{R}_k^{\mathbf{z}} \right)^{-1} \tag{23}$$
$$\mathbf{K}_k^{\theta} = \mathbf{P}_{k|k-1}^{\theta}\mathbf{\Gamma}_{k|k-1}^\intercal\mathcal{C}^\intercal (\mathcal{C}\mathbf{\Gamma}_{k|k-1}\mathbf{P}_{k|k-1}^{\theta}\mathbf{\Gamma}_{k|k-1}^\intercal\mathcal{C}^\intercal + \mathbf{R}_k^{\theta})^{-1} \tag{24}$$
$$\mathbf{\Gamma}_{k|k} = (\mathbf{I} - \mathbf{K}_k^{\mathbf{z}}\mathcal{C})\,\mathbf{\Gamma}_{k|k-1} \tag{25}$$

with the prediction update

$$\bar{\mathbf{z}}_{k+1|k} = \mathbf{F}_k\bar{\mathbf{z}}_{k|k} + \mathbf{E}_k + \mathcal{B}\mathbf{u}_k + \mathbf{\Psi}\bar{\theta}_{k|k} \tag{26}$$
$$\bar{\theta}_{k+1|k} = \bar{\theta}_{k|k} \tag{27}$$
$$\mathbf{P}_{k+1|k}^{\mathbf{z}} = \lambda_{\mathbf{z}}^{-1}\mathbf{F}_k \left(\mathbf{I} - \mathbf{K}_k^{\mathbf{z}}\mathcal{C} \right) \mathbf{P}_{k|k-1}^{\mathbf{z}}\mathbf{F}_k^\intercal \tag{28}$$
$$\mathbf{P}_{k+1|k}^{\theta} = \lambda_{\theta}^{-1} \left(\mathbf{I} - \mathbf{K}_k^{\theta}\mathcal{C}\mathbf{\Gamma}_{k|k-1} \right) \mathbf{P}_{k|k-1}^{\theta} \tag{29}$$
$$\mathbf{\Gamma}_{k+1|k} = \mathbf{F}_k\mathbf{\Gamma}_{k|k} - \mathbf{\Psi} \tag{30}$$

It was shown in [17] that the adaptive observer (12)-(15) coincides with the adaptive observer (21)-(30). It is worth noting that the structure of the proposed adaptive observer is reminiscent of other well-known state estimation techniques, such as the Kalman filter and Luenberger observer. However,

the observer is unique in that it has two observer gains, one associated with the state estimation $\mathbf{K}_k^{\mathbf{z}}$ and another with the parameter estimation $\mathbf{K}_k^{\theta}$. These two gains play a critical role in the observer's performance, and we allow for tuning of these gains using the parameters $\mathbf{R}_k^{\mathbf{z}}$ and $\mathbf{R}_k^{\theta}$. By adjusting these parameters, we can optimize the observer's performance and ensure that it is well-suited to the particular system being controlled. Furthermore, unlike the Kalman filter and Luenberger observer, our proposed observer is explicitly designed to be adaptive, meaning that it can adjust its parameters in real-time based on the available data. This feature allows the observer to maintain its accuracy and reliability even in the face of significant variations in the system's parameters or dynamics.

B. Proof of Stability

Theorem 3.1: Let the estimation errors be defined as

$$\tilde{\mathbf{z}}_k = \bar{\mathbf{z}}_{k|k} - \mathbf{z}_k \tag{31}$$

$$\tilde{\theta}_k = \bar{\theta}_{k|k} - \theta_k \tag{32}$$

Under *Assumptions 1-2*, the estimation errors $\tilde{\mathbf{z}}_k$ and $\tilde{\theta}_k$ tend to zero exponentially.

Proof: First, substituting (22) to (21), we have

$$\begin{aligned}\bar{\mathbf{z}}_{k|k} &= \bar{\mathbf{z}}_{k|k-1} + \mathbf{K}_k^{\mathbf{z}}\mathcal{C}(\mathbf{z}_k - \bar{\mathbf{z}}_{k|k-1}) \\ &\quad -\mathbf{\Gamma}_{k|k}(\bar{\theta}_{k|k} - \bar{\theta}_{k-1|k-1})\end{aligned} \tag{33}$$

Furthermore, substituting (33) into (31), yields

$$\begin{aligned}\tilde{\mathbf{z}}_k &= (\mathbf{I} - \mathbf{K}_k^{\mathbf{z}}\mathcal{C})\mathbf{F}_{k-1}\tilde{\mathbf{z}}_{k-1} + (\mathbf{I} - \mathbf{K}_k^{\mathbf{z}}\mathcal{C})\mathbf{\Psi}\tilde{\theta}_{k-1} \\ &\quad -\mathbf{\Gamma}_{k|k}(\tilde{\theta}_k - \tilde{\theta}_{k-1})\end{aligned} \tag{34}$$

Now consider the following error function

$$\mathbf{e}_k = \tilde{\mathbf{z}}_k + \mathbf{\Gamma}_{k|k}\tilde{\theta}_k \tag{35}$$

Utilizing (16) and (26), and substituting (34) into (35), the combined error is given by

$$\mathbf{e}_{k+1} = (\mathbf{I} - \mathbf{K}_{k+1}^{\mathbf{z}}\mathcal{C})\mathbf{F}_k\mathbf{e}_k \tag{36}$$

Under *Assumption 1-2*, $\mathbf{e}_k$ is exponentially stable. To check the convergence of the estimation error (31)-(32), substituting (22) and into (32), yields

$$\tilde{\theta}_{k+1} = \tilde{\theta}_k + \mathbf{K}_{k+1}^{\theta}\mathcal{C}\mathbf{F}_k\tilde{\mathbf{x}}_k + \mathbf{K}_{k+1}^{\theta}\mathcal{C}\mathbf{\Psi}\tilde{\theta}_k \tag{37}$$

Substituting (35) into (37), we have

$$\tilde{\theta}_{k+1} = \tilde{\theta}_k + \mathbf{K}_{k+1}^{\theta}\mathcal{C}\mathbf{F}_k\mathbf{e}_k - \mathbf{K}_{k+1}^{\theta}\mathcal{C}(\mathbf{F}_k\mathbf{\Gamma}_{k|k} - \mathbf{\Psi})\tilde{\theta}_k \tag{38}$$

and from (30), we have

$$\tilde{\theta}_{k+1} = (\mathbf{I} - \mathbf{K}_{k+1}^{\theta}\mathcal{C}\mathbf{\Gamma}_{k+1|k})\tilde{\theta}_k + \mathbf{K}_{k+1}^{\theta}\mathcal{C}\mathbf{F}_k\mathbf{e}_k \tag{39}$$

Since $\mathbf{K}_{k+1}^{\theta}$, $\mathcal{C}$, and $\mathbf{F}_k$ are bounded, then we can conclude that $\mathbf{K}_{k+1}^{\theta}$, $\mathcal{C}$, and $\mathbf{F}_k$ decays exponentially. Following Lemma 2.3 in [17], we can show that $\tilde{\theta}_k$ tends to zero exponentially. Since $\mathbf{e}_k$ is also exponentially stable, $\tilde{\mathbf{z}}_k$ goes to zero exponentially. ■

IV. NUMERICAL SIMULATIONS

This section presents the results of two simulations performed to evaluate the performance of our proposed observer. The first simulation illustrates the impact of sensor attacks on the trajectory of an autonomous mobile robot. The simulation shows how the robot deviates from its intended path due to these attacks, thereby highlighting the significance of our proposed observer in mitigating such effects. In the second simulation, we compared the performance of our proposed observer with an existing method that uses a stochastic approach. Our results indicate that our proposed observer outperforms the existing method by achieving higher accuracy and more efficient performance. This comparison provides empirical evidence for the efficacy of our proposed observer in enhancing the performance of autonomous mobile robots in the presence of sensor attacks. To this end, we consider a kinematic model of the autonomous mobile robot, which can be represented by a discrete-time model that incorporates time sampling Δt. Defining the state vector of the autonomous mobile robot as $\mathbf{x} = \begin{pmatrix} x & y & \psi & v & \delta \end{pmatrix}^{\mathsf{T}}$, the particularities of the model are described by the following equation:

$$\mathbf{x}_{k+1} = \begin{pmatrix} x_k \\ y_k \\ \psi_k \\ v_k \\ \delta_k \end{pmatrix} + \Delta t \left(\begin{pmatrix} v_k \cos\psi_k \\ v_k \sin\psi_k \\ \frac{v_k}{l}\tan\delta_k \\ 0 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ a_k \\ w_k \end{pmatrix} \right) \tag{40}$$

and the measurement equation subjected to sensor attack is

$$\mathbf{y}_k = \begin{pmatrix} x_k \\ y_k \end{pmatrix} + \begin{pmatrix} \theta_{1,k} \\ \theta_{2,k} \end{pmatrix}. \tag{41}$$

The position of the mobile robot in the xy-coordinate is represented by x_k and y_k, while its heading is denoted by ψ_k. The velocity of the mobile robot is denoted by v_k, while the steering angle is denoted by δ_k. The length of the robot is represented by l. The control inputs for the system are the acceleration a_k and the steering angular velocity ω_k. We assume we can only measure the position and the sensors that are to be targeted are those used to measure the robot's position in the x and y directions, affected by $\theta_{1,k}$ and $\theta_{2,k}$.

A. Comparison with and without Sensor Attacks

To assess the impact of spoofing on an autonomous mobile robot, we conducted a simulation consisting of two scenarios. The simulation was run for a duration of 60 seconds. In the first scenario, the mobile robot followed a predetermined trajectory from start to finish, without any interference or spoofing. This scenario served as a baseline for comparison purposes. In the second scenario, the robot was subjected to a spoofing attack that commenced 20 seconds after the simulation began, specifically at point $(20.7, -13.4)$. The spoofing was achieved by injecting a false signal into the robot's sensor system, which was assumed to be functioning without any faults. As a result of the attack, the robot's trajectory deviated from its original path, as can be observed in Figure 1. This scenario was designed to simulate the effect

of a real-world spoofing attack on the performance of an autonomous mobile robot. By conducting this simulation, we were able to evaluate the impact of spoofing attacks on the performance of autonomous mobile robot and identify potential vulnerabilities in the sensor systems. This finding provides valuable insights into the development of counter-measures to mitigate the impact of spoofing attacks on the performance of autonomous mobile robot.

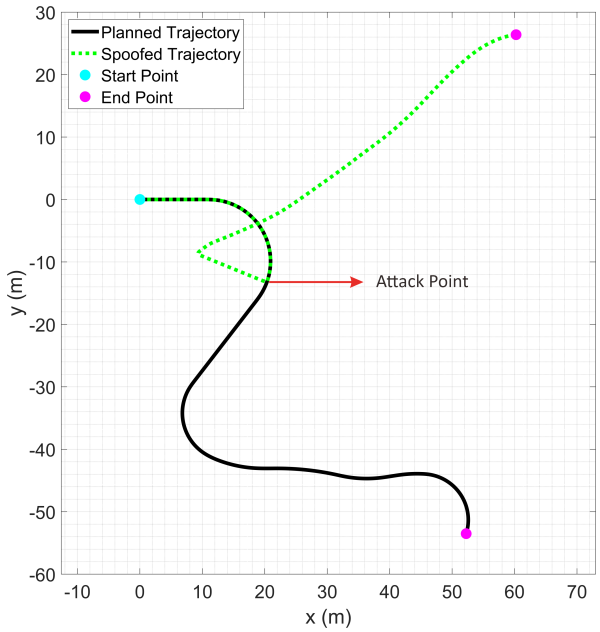

Fig. 1. Simulation of robot trajectory with and without sensor attacks.

B. Secure State Estimation based on the Adaptive Observer

The proposed adaptive observer (AO) for sensor attacks (21)-(22) is compared with the adaptive extended Kalman filter (AEKF) algorithm presented in [18]. The AEKF algorithm is started with the standard linear Kalman filter algorithm:

$$\mathbf{P}^f_{k+1|k} = \mathbf{F}_k\mathbf{P}^f_{k|k}\mathbf{F}_k^\intercal + \mathbf{Q}^f_k \quad (42)$$

$$\mathbf{\Sigma}_{k+1} = \mathcal{C}\mathbf{P}^f_{k+1|k}\mathcal{C}^\intercal + \mathbf{R}^f_k \quad (43)$$

$$\mathbf{K}^f_{k+1} = \mathcal{C}\mathbf{P}^f_{k+1|k}\mathbf{\Sigma}^{-1} \quad (44)$$

$$\mathbf{P}^f_{k+1|k+1} = (\mathbf{I}_n - \mathbf{K}^f_{k+1}\mathcal{C})\mathbf{P}^f_{k+1|k} \quad (45)$$

To estimate the state $\hat{\mathbf{z}}_k$ and parameters $\hat{\theta}_k$, the algorithm requires calculation of several auxiliary variables as follows:

$$\mathbf{\Upsilon}_{k+1} = (\mathbf{I}_n - \mathbf{K}^f_{k+1}\mathcal{C})\mathbf{F}_k\mathbf{\Upsilon}_k + (\mathbf{I}_n - \mathbf{K}^f_{k+1}\mathcal{C})\mathbf{\Psi} \quad (46)$$

$$\mathbf{\Omega}_{k+1} = \mathcal{C}\mathbf{F}_k\mathbf{\Upsilon}_k + \mathbf{\Psi} \quad (47)$$

$$\mathbf{\Lambda}_{K+1} = (\lambda\mathbf{\Sigma}_{k+1} + \mathbf{\Omega}_{k+1}\mathbf{S}_k\mathbf{\Omega}^\intercal_{k+1})^{-1} \quad (48)$$

$$\mathbf{\Pi}_{k+1} = \mathbf{S}_k\mathbf{\Omega}^\intercal_{k+1}\mathbf{\Lambda}_{k+1} \quad (49)$$

$$\mathbf{S}_{k+1} = \lambda^{-1}\mathbf{S}_k - \lambda^{-1}\mathbf{S}_k\mathbf{\Omega}^\intercal_{k+1}\mathbf{\Lambda}_{k+1}\mathbf{\Omega}_{k+1}\mathbf{S}_k \quad (50)$$

The estimated state $\hat{\mathbf{z}}_k$ and parameter $\hat{\theta}_k$ are given by:

$$\hat{\mathbf{z}}_{k+1} = \mathbf{F}_k\hat{\mathbf{z}}_k + \mathbf{E}_k + \mathcal{B}\mathbf{u}_k + \mathbf{\Psi}\hat{\theta}_k + \mathbf{K}^f_{k+1}\breve{\mathcal{Y}}_{k+1} + \mathbf{\Upsilon}_{k+1}\mathbf{\Pi}_{k+1}\breve{\mathcal{Y}}_{k+1} \quad (51)$$

$$\hat{\theta}_{k+1} = \hat{\theta}_k + \mathbf{\Pi}_{k+1}\breve{\mathcal{Y}}_{k+1} \quad (52)$$

where $\breve{\mathcal{Y}}_{k+1} = \mathcal{Y}_{k+1} - \mathcal{C}\hat{\mathbf{z}}_k$.

In this simulation, we set the sampling time Δt to 0.1 seconds, the length of the mobile robot l to 2 meters, and the matrix $\mathbf{\Psi}$ to the identity matrix $\mathbf{I}_2$. The spoofing attack on the sensor begins at 20 seconds and increases linearly over time. The adaptive observer's parameter values are given by: $\lambda_{\mathbf{x}} = 0.999$, $\lambda_\theta = 0.94$, $\mathbf{R}^{\mathbf{x}} = 10^7\mathbf{I}_2$, $\mathbf{R}^\theta = \mathbf{I}_2$, $\mathbf{P}^{\mathbf{x}}_0 = 0.01\mathbf{I}_7$, $\mathbf{P}^\theta_0 = 0.01\mathbf{I}_2$, and $\mathbf{A}_{\mathbf{f}} = 10\mathbf{I}_2$. Similarly, the parameter values for the AEKF are given by: $\lambda = 0.999$, $\mathbf{P}^f_0 = 0.01\mathbf{I}_7$, $\mathbf{Q}^f = \mathbf{I}_7$, $\mathbf{R}^f = 10^7\mathbf{I}_2$, and $\mathbf{S}_0 = 0.1\mathbf{I}_2$.

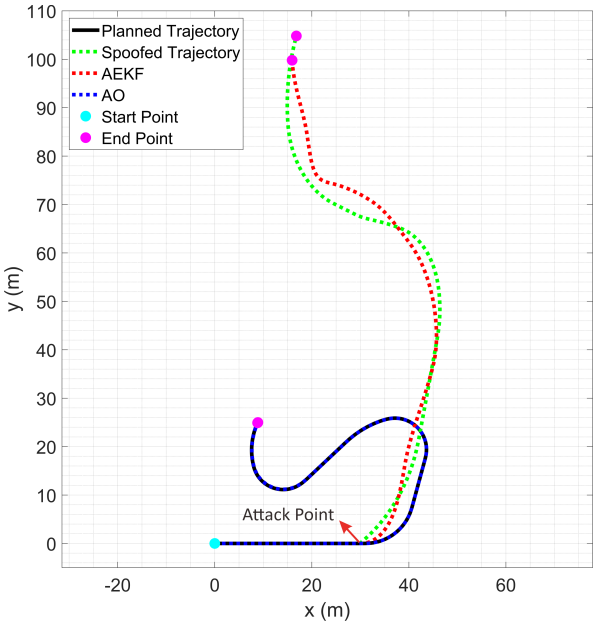

Fig. 2. Comparison of the planned trajectory, spoofed trajectory, and position estimation using AO and AEKF algorithms. The estimated position based on AO coincides with the planned trajectory.

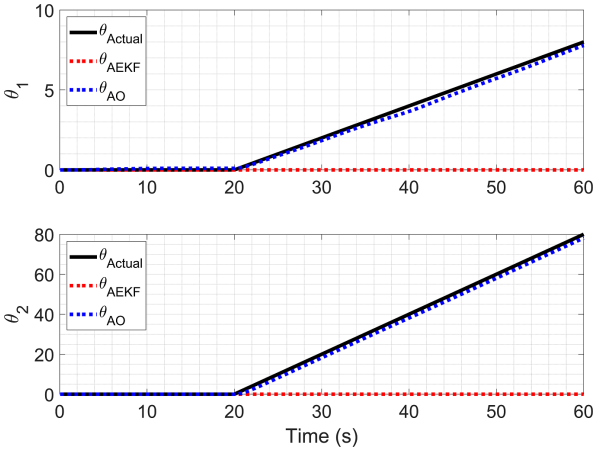

Fig. 3. Actual θ vs estimated θ using AO and AEKF algorithms.

The simulation results presented in Figure 2 demonstrate a clear difference between the AO and the AEKF algorithms. The black line in the figure represents the planned trajectory of the autonomous mobile robot. As the sensor attack is initiated at time 20s or at the point (30,0), the dotted green line represents the position measurements obtained from the attacked sensor. The AO's position estimation, depicted in the blue dot line, is almost identical to the planned trajectory, showing that the AO is an effective and secure state estimation algorithm. In contrast, the AEKF estimation is depicted in the dotted red line, and it follows the spoofed trajectory instead of the planned trajectory.

The magnitude value of the sensor attack is also estimated by the AO algorithm, as shown in Figure 3. The actual magnitude values of the sensor attack θ and the estimations obtained using the AO and AEKF algorithms are compared in the figure. The simulation results show that the AO algorithm accurately estimates both the state and magnitude of sensor attacks simultaneously. The AEKF algorithm, on the other hand, produces position estimations that deviate significantly from the true trajectory and tend to follow the measurements from the attacked sensor. After the position sensor is attacked, the estimated value of θ using AEKF remains at zero. The deviation of AEKF estimation from the actual trajectory is observed in the figure as well. Overall, the proposed AO algorithm yields estimations of position that closely approximate the true trajectory, even when the measurement data has been spoofed.

The robustness and accuracy of the AO algorithm make it a promising candidate for real-time implementation in practical systems. It can provide reliable state and magnitude estimation, which is particularly useful in safety-critical applications. On the other hand, the AEKF algorithm is less reliable in the presence of sensor spoofing, and it may not be suitable for safety-critical applications

V. CONCLUSIONS

The proposed observer for autonomous systems under sensor attacks has been successfully demonstrated through numerical simulations. The stability analysis of the observer has been rigorously proven, indicating that the observer is reliable for practical applications. Simulation results of a mobile robot, where its sensor is attacked by a spoofed signal, have been presented, and the proposed adaptive observer algorithm can successfully estimate the state and magnitude of sensor attacks. Using the proposed adaptive observer, the estimated position closely tracks the planned trajectory.

Future work can focus on the practical implementation of the observer for real-world systems. The effect of different types of sensor attacks can be further explored to improve the observer's robustness. Additionally, the observer's performance can be evaluated under different noise levels, sampling rates, and modeling uncertainties. Furthermore, extensions to the observer design for nonlinear and time-varying systems can be explored to enhance the observer's applicability. In addition, incorporating the observer into the system's control strategy can be investigated, leading to improved control performance in the presence of sensor attacks.

REFERENCES

[1] 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.

[2] 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.

[3] K. Kim, J. S. Kim, S. Jeong, J.-H. Park, and H. K. Kim, "Cybersecurity for autonomous vehicles: Review of attacks and defense," *Computers & Security*, vol. 103, p. 102150, 2021.

[4] 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.

[5] Y.-C. Liu, G. Bianchin, and F. Pasqualetti, "Secure trajectory planning against undetectable spoofing attacks," *Automatica*, vol. 112, p. 108655, 2020.

[6] M. Jeyaselvi, M. Sathya, S. Suchitra, S. Jafar Ali Ibrahim, and N. S. Kalyan Chakravarthy, "Svm-based cloning and jamming attack detection in iot sensor networks," in *Advances in Information Communication Technology and Computing*, V. Goar, M. Kuri, R. Kumar, and T. Senjyu, Eds. Singapore: Springer Nature Singapore, 2022, pp. 461–471.

[7] D. Ding, Q.-L. Han, X. Ge, and J. Wang, "Secure state estimation and control of cyber-physical systems: A survey," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 51, no. 1, pp. 176–190, 2021.

[8] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure state-estimation for dynamical systems under active adversaries," in *2011 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2011, pp. 337–344.

[9] L. An and G.-H. Yang, "Secure state estimation against sparse sensor attacks with adaptive switching mechanism," *IEEE Transactions on Automatic Control*, vol. 63, no. 8, pp. 2596–2603, 2018.

[10] W. Ao, Y. Song, and C. Wen, "Distributed secure state estimation and control for cpss under sensor attacks," *IEEE Transactions on Cybernetics*, vol. 50, no. 1, pp. 259–269, 2020.

[11] S. Mishra, Y. Shoukry, N. Karamchandani, S. Diggavi, and P. Tabuada, "Secure state estimation: Optimal guarantees against sensor attacks in the presence of noise," in *2015 IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 2929–2933.

[12] 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.

[13] Y. Shoukry, M. Chong, M. Wakaiki, P. Nuzzo, A. Sangiovanni-Vincentelli, S. A. Seshia, J. P. Hespanha, and P. Tabuada, "Smt-based observer design for cyber-physical systems under sensor attacks," *ACM Trans. Cyber-Phys. Syst.*, vol. 2, no. 1, 2018.

[14] Y. H. Chang, Q. Hu, and C. J. Tomlin, "Secure estimation based kalman filter for cyber–physical systems against sensor attacks," *Automatica*, vol. 95, pp. 399–412, 2018.

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

[16] A. Ţiclea and G. Besançon, "Exponential forgetting factor observer in discrete time," *Systems & Control Letters*, vol. 62, no. 9, pp. 756–763, 2013.

[17] ——, "Adaptive observer design for discrete time ltv systems," *International Journal of Control*, vol. 89, no. 12, pp. 2385–2395, 2016.

[18] Q. Zhang, "Adaptive kalman filter for actuator fault diagnosis," *Automatica*, vol. 93, pp. 333–342, 2018.