Hindawi
Security and Communication Networks
Volume 2021, Article ID 5572186, 12 pages
https://doi.org/10.1155/2021/5572186

Research Article

UKF-Based Vehicle Pose Estimation under Randomly Occurring Deception Attacks

Xinghua Liu,[1] **Dandan Bai**,[1] **Yunling Lv**,[1] **Rui Jiang**,[2] **and Shuzhi Sam Ge**[2]

[1]*Department of Power Grid Information and Control Engineering, School of Electrical Engineering, Xi'an University of Technology, Xi'an 710048, China*
[2]*Department of Electrical and Computer Engineering, National University of Singapore, Singapore 117583*

Correspondence should be addressed to Rui Jiang; rui_jiang@u.nus.edu

Received 27 February 2021; Accepted 6 September 2021; Published 24 September 2021

Academic Editor: Stelvio Cimato

Considering various cyberattacks aiming at the Internet of Vehicles (IoV), secure pose estimation has become an essential problem for ground vehicles. This paper proposes a pose estimation approach for ground vehicles under randomly occurring deception attacks. By modeling attacks as signals added to measurements with a certain probability, the attack model has been presented and incorporated into the existing process and measurement equations of ground vehicle pose estimation based on multisensor fusion. An unscented Kalman filter-based secure pose estimator is then proposed to generate a stable estimate of the vehicle pose states; i.e., an upper bound for the estimation error covariance is guaranteed. Finally, the simulation and experiments are conducted on a simple but effective single-input-single-output dynamic system and the ground vehicle model to show the effectiveness of UKF-based secure pose estimation. Particularly, the proposed scheme outperforms the conventional Kalman filter, not only by resulting in more accurate estimation but also by providing a theoretically proved upper bound of error covariance matrices that could be used as an indication of the estimator's status.

1. Introduction

With the continuous development of Artificial Intelligence (AI), Internet of Things (IoT), and high-performance computing devices in intelligent transportation systems [1], autonomous vehicles (AVs) have become one of the focus research topics in the last decade. Implemented with AV technologies, transportation safety and efficiency have been greatly improved by reducing drivers' workload, optimizing resource allocation, alleviating traffic congestion, and minimizing vehicle energy consumption. For AVs, it is essential to accurately measure their pose (namely, translation and rotation) and speed in real time for accurate monitoring, path planning, behavioral decision-making, and control [2, 3]. However, the inherent and tight connection between AVs and networks makes AVs vulnerable targets of cyberattacks. Therefore, secure pose estimation under attacks has become a crucial problem worth studying.

Vehicle pose estimation is a complex and challenging task, which has attracted much attention in recent years. Particularly, for a small Unmanned Aerial Vehicle (UAV), a 3D local pose estimation system has been presented in [4] where the system is realized by fusing 3D position estimations using a loosely coupled extended Kalman filter (EKF) architecture. The data come from an ultra-wideband transceiver network, an inertial measurement unit sensor, and a barometric pressure sensor. Pose estimation with state or measurement constraints has been frequent in AV navigation. In view of the inherent constraints, a formulation based on the dynamic potential field has been proposed in [5] to express states, measurements, and constraints on connected Riemannian manifolds, and then, an information fusion scheme of dynamic potential field system based on multisensor measurement and constraints is designed. It is worth noting that in recent years, due to the fusion of multiple sensors, estimation results are more vulnerable to frequent attacks. Liu et al. [6] discussed the AV secure pose

estimation problem under cyberattacks to deal with the possible sensor attacks, and an EKF reconfiguration scheme has been designed to mitigate the influence of sensor attacks.

In the existing research, sensor attacks mainly include Denial of Service (DoS) attacks [7] and deception attacks [8]. DoS attacks are one of the common attack methods used by hackers, who try to make the target machine stop providing services. Deception attacks mean that the attacker can rearrange the data in the system to make the sensor or controller receive false data, thus causing the system to fail to function normally. By using a set of random variables of Bernoulli distribution to describe randomly deception attacks, a coupled unscented Kalman filter (UKF) has been proposed [9] to propagate the sigma points of the UKF by introducing the coupled terms, and the recursive filtering problem of a class of complex discrete time networks with random deception attacks has been studied. In [10], the position sensor deception attack detection and estimation problem is investigated for a local vehicle in a vehicle platoon. A linearized model has been presented to describe the longitudinal dynamics of a local vehicle. In [7], it is proposed that the attacker behavior is limited only by the frequency and duration of DoS attacks. If the communication links used by the sensor to receive neighbor information lose packet due to DoS attacks, the sensor will give up location estimation. In our paper, we further assume that the sensor is subject to random deception attacks with a given probability. This paper focuses on modeling the AV pose estimation problem with attacks and secure estimation of vehicles' poses in a 2D plane. Distinguished from the conventional Kalman filter, an unscented Kalman filter-inspired secure recursive estimator is designed to provide estimation, allowing for possible attacks on sensors. By solving several matrix difference equations, the upper bound of estimation error covariance is guaranteed and correctly updated during the recursive process. The contributions are summarized as follows:

(1) The modeling of the system takes the occurrence of random deception attacks into account, such that the secure dynamic pose estimation problem has been formulated for autonomous vehicles

(2) The proposed unscented Kalman-type secure recursive estimator provides a theoretically proved upper bound for error covariance matrices with stable and efficient state estimation

(3) The feasibility and effectiveness of the proposed approach are verified in both a simulated model and the practical AV system, where single and multiple attacks have been considered in experimental design

Notation 1. The following notations are used throughout this paper. We use $\mathbb{R}^n$ to denote the n dimensional Euclidean space, and $\mathbb{R}^{m\times n}$ represents the set of all $m \times n$ matrices. $\mathbb{E}$ denotes the mathematical expectation operator of an underlying probability space, which will be clear from the context. $A > B$ implies that both A and B are symmetric and $A - B$ is positive definite. We let I be the identity matrix with proper dimensions. Let $\|X\|$ and $\|A\|$ be the Euclidean norm of a vector x and a matrix A, respectively. The superscripts T and -1 denote matrix transposition and matrix inverse, respectively. The remainder of this paper is organized as follows: Section 2 summarizes related work in secure state estimation in cyberphysical systems. Section 3 presents the system model and attack model for ground autonomous vehicle pose estimation problem. The estimator design and mathematical proof are presented in Section 4, followed by Section 5 that shows simulation results for an illustrative Single-Input and Single-Output (SISO) system. Experimental validation and results are shown in Section 6. Finally, Section 7 concludes the paper.

2. Related Work

Cyberphysical System (CPS) is a complex system with integrated computing, networking, and physical environment. As the interaction between physical and network systems increases, CPS becomes more vulnerable to network attacks. Some achievements have been made in secure dynamic state estimation under sensor attacks [11, 12]. In [12], the state estimation problem of a linear dynamic system is considered when the measurement data of some sensors are damaged by attackers. In [13], when the unknown subset of the sensor is destroyed by the enemy arbitrarily, a secure state estimation algorithm is proposed, and the upper bound of the reachable state estimation error of the is given.

CPS plays an important role in many fields. In intelligent transportation, regarding AV pose estimation, the relative pose of AV when driving in a highly dynamic and possibly chaotic environment was studied in [14], where a relative pose estimation algorithm based on multiple nonoverlapping cameras is proposed, and the algorithm is robust even when the number of outliers is overwhelming. In [15], an enabling multisensor fusion-based longitudinal vehicle speed estimator was proposed for four-wheel-independently actuated electric vehicles using a Global Positioning System and BeiDou Navigation Positioning (GPS-BD) module and a low-cost inertial measurement unit (IMU). Liu et al. [16] presented a comprehensive evaluation of state-of-the-art sideslip angle estimation methods, with the primary goal of quantitatively revealing their strengths and limitations. Wang et al. [17] focused on providing an LTR evaluation system that adopts an IMU as the signal input. Unfortunately, there is less attention on the AV secure pose estimation problem. In our previous work [18], a secure dynamic pose estimation method based on the filter has been proposed to make the vehicle pose resilient to possible sensor attacks. When all sensors on autonomous vehicles are benign, the proposed estimator is consistent with the conventional Kalman filtering. On this basis, a vehicle pose estimation based on an unscented Kalman filter under sensor attacks is proposed in this paper. Compared with other estimators, the proposed estimator in this paper still follows the framework of KF, but the next state prediction becomes the expansion and nonlinear mapping of the sigma point set. This method has two advantages: (1) the possible complex operation during Jacobian matrix computation for

the nonlinear process equation could be avoided; (2) the approach has better generality in advanced nonlinear systems, including those without explicit Jacobian formulation.

In our paper, we consider the impact of randomly occurring deception attacks (possible sensor attacks) in the design of a secure dynamic pose estimator for AV. By utilizing the unscented Kalman filter algorithm combined with matrix inequality techniques, we propose a secure recursive estimation algorithm and derive an upper bound of estimation error covariance by selected optimal estimator parameters. Moreover, the proposed approach can be implemented efficiently in real time and is suitable for recursive computation in applications with limited computational capability.

3. Pose Estimation Problem for Ground Vehicles under Attacks

In this section, we present the process model, measurement model, and attack model such that the ground vehicle pose estimation problem can be formulated. Although the problem has been modeled in our previous work [18], we still formulate it here for completeness and readers' convenience.

3.1. System Model. Consider the following discrete state space model for generality:

$$x_{k+1} = f(x_k) + h(u_k) + w_k, \tag{1}$$

$$z_k = g(x_k) + v_k, \tag{2}$$

where k denotes time index; $\mathbf{f}(\cdot)$ and $\mathbf{g}(\cdot)$ are nonlinear process and measurement functions, respectively; and $\mathbf{h}(\mathbf{u}_k)$ is a stochastic function satisfying $\mathbb{E}\{\mathbf{h}(\mathbf{u}_k)|\mathbf{x}_k\} = 0$ for all $\mathbf{x}_k$. $\mathbf{w}_k \sim \mathcal{N}(0, \mathbf{Q})$ and $\mathbf{v} \sim \mathcal{N}(0, \mathbf{R})$ denote independent and identically distributed (i.i.d.) Gaussian process and measurement noises with zero mean and covariance matrices $\mathbf{Q} > 0$ and $\mathbf{R} > 0$, respectively.

Two 3D reference frames are used in system modeling: the global frame and the local frame. The global frame (sometimes called the "world frame") plays the role of a map, on which the vehicle needs to be localized; the local frame (or "body frame") moves along the vehicle, which is usually the reference of local sensors such as wheel encoder and inertial measurement unit (IMU). The pose estimation problem aims to estimate the translation and rotation of the local frame with respect to the global frame. As we focus on ground vehicles, projections from 3D to 2D could be applied to reduce the complexity of the model, by following certain assumptions [19]. Particularly, the states are defined as

$$x = [x \quad y \quad v \quad \psi \quad \dot{\beta}]^T, \tag{3}$$

where x, y, and ψ are coordinates of vehicle position and the heading on global $x - y$ plane; v denotes the projection of vehicle translational velocity onto the local y axis; and $\dot{\beta}$ represents the rotational velocity with respect to the local z axis. In other words, v and $\dot{\beta}$ indicate the forward and rotating velocities that correspond to the vehicle's two manipulating modes: throttle and steering. We further define the control input $\mathbf{u} = [u_v, u_{\dot{\beta}}]^\top$ that feeds throttle and steering into the system motion model.

By incorporating the above state definition into the vehicle's motion model (1), we have

$$\begin{bmatrix} x \\ y \\ v \\ \psi \\ \dot{\beta} \end{bmatrix}_{k+1} = \begin{bmatrix} x - v(\Delta t \sin \psi) \\ y + v(\Delta t \cos \psi) \\ v + u_v \Delta t \\ \psi + \dot{\beta}\Delta t \\ \dot{\beta} + u_{\dot{\beta}}\Delta t \end{bmatrix}_k + w_k. \tag{4}$$

As for the specific formulation of the measurement equation (2), we consider a common configuration of sensors [19] that measure (translational and rotational) pose x, y, ψ, forward velocity v, and steering angle α as follows:

$$z_k = \begin{bmatrix} z_x \\ z_y \\ z_v \\ z_\psi \\ z_\alpha \end{bmatrix}_k = \begin{bmatrix} x \\ y \\ v \\ \psi \\ \tan^{-1}\left(\dfrac{L\dot{\beta}}{v}\right) \end{bmatrix}_k + v_k, \tag{5}$$

where L denotes the wheelbase between the front and rear wheels of the vehicle. The measurement can be obtained from the combination of global pose estimation sensors such as satellite navigation systems, visual odometry, or Attitude and Heading Reference Systems (AHRS), and local sensors including wheel encoders and steering angle sensors.

In the circumstance where the linear approximation of measurement equation is required, the Jacobian matrix $\mathbf{G}_k = \partial \mathbf{g}(\mathbf{x})/\partial \mathbf{x}|_{\mathbf{x}=\mathbf{x}_k}$, which needs to be computed at each iteration, can be used for linearization:

$$g(x_k) \approx g(x_0) + G_k(x_k - x_0). \tag{6}$$

Note that only the measurement of α is nonlinear, and α is mostly zero with small fluctuations. By selecting $\mathbf{x}_0 = 0$ as the point of interest where $\mathbf{g}(\mathbf{x}_0) = 0$, we have the approximated linear time-varying form of measurement equation as

$$z_k = G_k x_k + v_k. \tag{7}$$

3.2. Attack Model. In this paper, we assume that the sensors are subject to randomly occurring deception attacks with a given probability. The attack model is described as follows:

$$\tilde{z}_k = z_k + \gamma_k a_k = G_k x_k + v_k + \gamma_k a_k, \tag{8}$$

where $\tilde{\mathbf{z}}_k$ denotes the measurement with possible attacks, $\mathbf{a}_k$ denotes the information sent by attacks, and γ_k is a stochastic variable.

Before giving the deception attack model, we make some further assumptions on the system knowledge that are possessed by the adversary for implementing a successful attack. In this paper, it is assumed that the adversary has sufficient resources and adequate knowledge to arrange a successful attack $\mathbf{a}_k$.

The information $\mathbf{a}_k$ caused by deception attacks can be regarded as $\mathbf{a}_k = -\mathbf{z}_k + \xi_k$ where the nonzero ξ_k satisfying $\|\xi_k\| \le \delta$ is an arbitrary energy-bounded signal. The stochastic variable γ_k is a Bernoulli distributed white sequence taking values on $\{0, 1\}$ with probabilities

$$\Pr\{\gamma_k = 0\} = \overline{\gamma},\ \Pr\{\gamma_k = 1\} = 1 - \overline{\gamma}, \tag{9}$$

where $\overline{\gamma} \in (0, 1]$ is a known constant. More detailed explanations can be found in [20].

Remark 1. The attack model has the ability to describe the randomly occurring deception attacks; that is, the stochastic variable $\gamma_k$is utilized to govern the random nature of sensor attacks on autonomous vehicles. The false data sent by deception attackers could be identified by using some algorithms and some hardware and software tools. According to the definition of frequentist probability, we may deduce the value of $\overline{\gamma}$ in applications. Hence, the given Bernoulli distribution can properly reveal the random nature of deception attacks.

To derive the main result of this paper, we will employ the following lemma.

Lemma 1 (see [21]). *For any dimension-compatible matrices* $\mathbf{D}$, $\mathbf{E}$, *and a scalar* $\varepsilon > 0$, *the following inequality holds:*

$$DE + E^{\top}D^{\top} \le \varepsilon\, DD^{\top} + \varepsilon^{-1}\, EE^{\top}. \tag{10}$$

4. Estimator Design

4.1. Design of the Unscented Kalman Filter. The UKF uses unscented transformation (UT) to represent a random variable by using a number of deterministically selected sample points (called sigma points). These points capture the mean and covariance of the random variable and, when propagated through the true nonlinear system, capture the posterior mean and covariance accurately.

Denote the one-step prediction error and the estimation error as $\mathbf{e}_{k+1|k} = \mathbf{x}_{k+1} - \hat{\mathbf{x}}_{k+1|k}$ and $\mathbf{e}_k = \mathbf{x}_k - \hat{\mathbf{x}}_k$, respectively. The one-step prediction error covariance matrix $\mathbf{P}_{k+1|k}$ and the estimation error covariance matrix $\mathbf{P}_{k+1}$ can be obtained as follows:

$$P_{k+1|k} = \mathbb{E}\left\{\left[x_{k+1} - \hat{x}_{k+1|k}\right]\left[x_{k+1} - \hat{x}_{k+1|k}\right]^{\mathrm{T}}\right\}, \tag{11a}$$

$$P_{k+1} = \mathbb{E}\left\{\left[x_{k+1} - \hat{x}_{k+1}\right]\left[x_{k+1} - \hat{x}_{k+1}\right]^{\top}\right\}. \tag{11b}$$

We are now ready to conduct the one-step prediction error matrix in terms of the solvability of recursive Riccati difference equations and obtain the parameter gain matrix of the unscented Kalman filter, which is developed in the following theorem.

Theorem 1. *Consider the discrete kinematic equation (1) suffering from attacks as (8). For any given positive constants* ε_k, $k = 0, 1, 2, \ldots$, *and the initial condition* $\mathbf{x}_0$, $\hat{\mathbf{x}}_0 = \mathbb{E}\{\mathbf{x}_0\}$, $\Pi_0 = \mathbf{P}_0$, $\Sigma_0 = \mathbb{E}\{\mathbf{x}_0\mathbf{x}_0^{\top}\}$, *we can derive that the parameter gain matrix of unscented Kalman filter is given as follows:*

$$K_{k+1} = \alpha_4 P_{k+1|k} G_k^{\top}\left[\alpha_1 G_k P_{k+1|k} G_k^{\top} + \alpha_2 G_k \Sigma_{k+1} G_k^{\top} + \alpha_3 I + R\right]^{-1}, \tag{12}$$

where $\alpha_1 = [1 + (1 - \overline{\gamma})\varepsilon_k]\overline{\gamma}^2$, $\alpha_2 = \overline{\gamma}(1 - \overline{\gamma})(1 + \varepsilon_k)$, $\alpha_3 = (1 - \overline{\gamma}^2)\varepsilon_k^{-1}\delta^2 + (1 - \overline{\gamma})\delta^2$, *and* $\alpha_4 = \overline{\gamma} + (\overline{\gamma} - \overline{\gamma}^2)\varepsilon_k$. *The upper bound for the estimation error covariance is* Π_{k+1}, *which can be recursively calculated by equation (23).*

Proof.

Step 1: initialization.

To calculate the statistics of a random variable that undergoes a nonlinear transformation, a matrix χ is generated using $2n + 1$ weighted **sigma points**. The computation algorithm begins with the initial conditions:

$$\begin{aligned} &\hat{x}_0 = \mathbb{E}\{x_0\}, \\ &P_0 = \mathbb{E}\left\{\left(x_0 - \hat{x}_0\right)\left(x_0 - \hat{x}_0\right)^{\top}\right\}. \end{aligned} \tag{13}$$

Step 2: generation of sigma points.

We calculate UT sampling as follows:

$$\begin{cases} \chi_{i,k|k} = \hat{x}_{k|k}, & i = 0, \\ \chi_{i,k|k} = \hat{x}_{k|k} + \left(\sqrt{(n+\lambda)P_{k|k}}\right)_i, & i = 1, 2, \ldots, n, \\ \chi_{i,k|k} = \hat{x}_{k|k} - \left(\sqrt{9n + \lambda P_{k|k}}\right)_i, & i = n+1, \ldots, 2n, \end{cases}$$

$$\begin{cases} \omega_i^{(m)} = \dfrac{\lambda}{n+\lambda}, & i = 0, \\ \omega_i^{(c)} = \dfrac{\lambda}{n+\lambda} + \left(1 - \alpha^2 + \beta\right), & i = 0, \\ \omega_i^{(m)} = \omega_i^{(c)} = \dfrac{1}{2(n+\lambda)}, & i = 1, 2, \ldots, 2n, \end{cases} \tag{14}$$

where $\lambda = \alpha^2(n + \kappa) - n, \alpha$ is the proportion factor, and the distribution distance of particles can be adjusted by changing the value of α to reduce the error. Parameters κ and β can be tuned and are generally set to 0 and 2, respectively. $(\sqrt{(n+\lambda)P_{k|k}})_i$ is the i-th column of the square root of the matrix, $\omega_i^{(m)}$ is the

weighted mean, and $\omega_i^{(c)}$ is the weighted covariance.

Step 3: one-step prediction is made for sigma sampling points to get the state prediction value and prediction covariance of each particle. First, we calculated the state prediction value as follows:

$$\chi_{i,k+1|k} = f\left(\chi_{i,k|k}\right), \tag{15a}$$

$$\hat{x}_{k+1|k} = \sum_{i=0}^{2n} \omega_i^{(m)} \chi_{i,k+1|k}. \tag{15b}$$

And from (11a), we know that

$$P_{k+1|k} = \sum_{i=0}^{2n} \omega_i^{(c)} \left[\chi_{i,k+1|k} - \hat{x}_{k+1|k}\right]\left[\chi_{i,k+1|k} - \hat{x}_{k+1|k}\right]^{\top} + Q. \tag{16}$$

Then, we have

$$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}\left(\tilde{z}_{k+1} - \overline{\gamma} G_k \hat{x}_{k+1|k}\right)\hat{x}_{k+1|k} + K_{k+1}\left(G_k x_{k+1} + v_{k+1} + \gamma_{k+1} a_{k+1} - \overline{\gamma} G_k \hat{x}_{k+1|k}\right). \tag{17}$$

Step 4: posterior error.

Since $e_k = x_k - \hat{x}_k$, and if we plug in $a_{k+1} = -G_k x_{k+1} - v_{k+1} + \xi_{k+1}$, it can be obtained that

$$\begin{aligned} e_{k+1} &= x_{k+1} - \hat{x}_{k+1} \\ &= x_{k+1} - \hat{x}_{k+1|k} - K_{k+1}\left(G_k x_{k+1} + v_{k+1} + \gamma_{k+1} a_{k+1} - \overline{\gamma} G_k \hat{x}_{k+1|k}\right) \\ &= \left(I - \overline{\gamma} K_{k+1} G_k\right) e_{k+1|k} - K_{k+1}\left(\gamma_{k+1} a_{k+1} + v_{k+1} + (1 - \overline{\gamma}) G_k x_{k+1}\right) \\ &= \left(I - \overline{\gamma} K_{k+1} G_k\right) e_{k+1|k} - K_{k+1}\left(-\gamma_{k+1} \times G_k x_{k+1} - \gamma_{k+1} v_{k+1} + \gamma_{k+1} \xi_{k+1} + v_{k+1} + (1 - \overline{\gamma}) G_k x_{k+1}\right). \end{aligned} \tag{18}$$

Step 5 : posterior covariance.

From (11b), we know that

$$\begin{aligned} P_{k+1} &= \mathbb{E}\{e_{k+1} e_{k+1}^{\top}\} \\ &= \mathbb{E}\Big\{\Big[\left(I - \overline{\gamma} K_{k+1} G_k\right) e_{k+1|k} - K_{k+1}\left(-\gamma_{k+1} G_k x_{k+1} - \gamma_{k+1} v_{k+1} + \gamma_{k+1} \xi_{k+1} + v_{k+1} + (1 - \overline{\gamma}) \times G_k x_{k+1}\right)\Big] \\ &\quad \cdot \Big[\left(I - \overline{\gamma} K_{k+1} G_k\right) e_{k+1|k} - K_{k+1} \times \left(-\gamma_{k+1} G_k x_{k+1} - \gamma_{k+1} v_{k+1} + \gamma_{k+1} \xi_{k+1} + v_{k+1} + (1 - \overline{\gamma}) G_k x_{k+1}\right)\Big]^{\top}\Big\}. \end{aligned} \tag{19}$$

Then, we can obtain that

$$\begin{aligned} P_{k+1} = {} & \left(I - \overline{\gamma} K_{k+1} G_k\right) P_{k+1|k} \left(I - \overline{\gamma} K_{k+1} G_k\right)^{\top} - (1 - \overline{\gamma})\left(I - \overline{\gamma} K_{k+1} G_k\right) \mathbb{E}\left\{e_{k+1|k} \xi_{k+1}^{\top}\right\} K_{k+1}^{\top} \\ & - (1 - \overline{\gamma}) K_{k+1} \mathbb{E}\left\{\xi_{k+1} e_{k+1\,|\,k}^{\top}\right\} \left(I - \overline{\gamma} K_{k+1} G_k\right)^{\top} \\ & - \overline{\gamma}(1 - \overline{\gamma}) K_{k+1} G_k \mathbb{E}\{x_{k+1} \xi_{k+1}^{\top}\} K_{k+1}^{\top} \\ & - \overline{\gamma}(1 - \overline{\gamma}) K_{k+1} \mathbb{E}\{\xi_{k+1} x_{k+1}^{\top}\} G_k^{T} K_{k+1}^{\top} \\ & + \overline{\gamma}(1 - \overline{\gamma}) K_{k+1} G_k \mathbb{E}\{x_{k+1} x_{k+1}^{\top}\} G_k^{\top} K_{k+1}^{\top} + (1 - \overline{\gamma}) K_{k+1} \xi_{k+1} \xi_{k+1}^{\top} K_{k+1}^{\top} \\ & + \overline{\gamma} K_{k+1} R K_{k+1}^{\top}. \end{aligned} \tag{20}$$

By Lemma 1 and applying the property of matrix trace, we have that

Step 1. Initialization:
(1) Set the values of initial pose state $\mathbf{x}_0$, initial estimate state $\hat{\mathbf{x}}_0$, initial estimation error covariance matrix $\mathbf{P}_0$, and initial state covariance matrix Σ_0
(2) Set the value of $\overline{\gamma}$ and determine the value of δ (the norm bound of arbitrary signal ξ_k)
(3) Set the control input signal $\mathbf{u}_k$, i.e., translational and rotational acceleration for the autonomous vehicle
(4) Let $\Pi_0 = \mathbf{P}_0$ and choose the proper ε_k for all k to calculate α_1, α_2, α_3, and α_4
(5) Set discrete time index $k = 0$

Step 2. State covariance matrix Σ_{k+1} is updated as follows:
$\Sigma_{k+1} = \sum_{i=0}^{2n} \omega_i^{(c)} (\chi_{i,k+1|k} \cdot \chi_{i,k+1|k}^{\top}) + h(u_k)h(u_k)^{\top} + Q.$

Step 3. The secure recursive estimator gain $\mathbf{K}_{k+1}$ and Π_{k+1} are calculated as follows:
$K_{k+1} = \alpha_4 P_{k+1|k} G_k^{\top} [\alpha_1 G_k P_{k+1|k} G_k^{\top} + \alpha_2 G_k \Sigma_{k+1} G_k^{\top} + \alpha_3 I + R]^{-1},$
$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}(\tilde{z}_{k+1} - \overline{\gamma} G_k \hat{x}_{k+1|k}) = \hat{x}_{k+1|k} + K_{k+1}(G_k x_{k+1} + v_{k+1} + \gamma_{k+1} a_{k+1} - \overline{\gamma} G_k \hat{x}_{k+1|k})$
$K_{k+1} = \alpha_4 P_{k+1|k} G_k^{\top} [\alpha_1 G_k P_{k+1|k} G_k^{\top} + \alpha_2 G_k \Sigma_{k+1} G_k^{\top} + \alpha_3 I + R]^{-1},$
$\hat{x}_{k+1} = \hat{x}_{k+1|k} + K_{k+1}(\tilde{z}_{k+1} - \overline{\gamma} G_k \hat{x}_{k+1|k})$
$= \hat{x}_{k+1|k} + K_{k+1}(G_k x_{k+1} + v_{k+1} + \gamma_{k+1} a_{k+1} - \overline{\gamma} G_k \hat{x}_{k+1|k})$

Step 4. Set $k = k + 1$ and go to Step 2.

Algorithm 1: UKF-based secure recursive estimator.

$$\begin{aligned}
P_{k+1} \le{}& (I - \overline{\gamma} K_{k+1} G_k) P_{k+1|k} (I - \overline{\gamma} K_{k+1} G_k)^{\top} \\
&- (1 - \overline{\gamma}) \left[\varepsilon_k (I - \overline{\gamma} K_{k+1} G_k) \mathbb{E}\left(e_{k+1} e_{k+1}^{T}\right) \right. \\
&\times (I - \overline{\gamma} K_{k+1} G_k)^{T} + \varepsilon_k^{-1} \delta^2 K_{k+1} K_{k+1}^{\top} \left. \right] \\
&- \overline{\gamma}(1 - \overline{\gamma}) K_{k+1} \left[\varepsilon_k G_k \Sigma_{k+1} G_k^{T} + \varepsilon_k^{-1} \delta^2 \right] \\
&- \overline{\gamma}(1 - \overline{\gamma}) K_{k+1} \left[\varepsilon_k G_k \Sigma_{k+1} G_k^{T} + \varepsilon_k^{-1} \delta^2 \right] \\
&\times K_{k+1}^{\top} + \overline{\gamma}(1 - \overline{\gamma}) K_{k+1} G_k \Sigma_{k+1} G_k^{T} K_{k+1}^{\top} \\
&+ (1 - \overline{\gamma}) K_{k+1} \delta^2 K_{k+1}^{\top} + \overline{\gamma} K_{k+1} R K_{k+1}^{\top}, \\
={}& \left[1 + (1 - \overline{\gamma})\varepsilon_k\right] (I - \overline{\gamma} K_{k+1} G_k) P_{k+1|k} (I - \overline{\gamma} K_{k+1} G_k)^{\top} \\
&+ \left[\overline{\gamma}(1 - \overline{\gamma})(1 + \varepsilon_k)\right] K_{k+1} G_k \Sigma_{k+1} G_k^{\top} K_{k+1}^{\top} \\
&+ \left[\left(1 - \overline{\gamma}^2\right)\varepsilon_k^{-1} \delta^2 + (1 - \overline{\gamma})\delta^2\right] K_{k+1} K_{k+1}^{\top} \\
&+ \overline{\gamma} K_{k+1} R K_{k+1}^{\top},
\end{aligned} \tag{21}$$

where

$$\begin{aligned}
\Sigma_{k+1} &= \mathbb{E}\{x_{k+1} x_{k+1}^{\top}\} \\
&= \mathbb{E}\left\{\left(f(x_k) + h(u_k) + w_k\right)\left(f(x_k) + h(u_k) + w_k\right)^{\top}\right\} \\
&= \sum_{i=0}^{2n} \omega_i^{(c)} \left(\chi_{i,k+1|k} \cdot \chi_{i,k+1|k}^{\top}\right) + h(u_k) h(u_k)^{\top} + Q.
\end{aligned} \tag{22}$$

Define

$$\begin{aligned}
\Pi_{k+1} = {}& \left[1 + (1 - \overline{\gamma})\varepsilon_k\right] (I - \overline{\gamma} K_{k+1} G_k) P_{k+1|k} (I - \overline{\gamma} K_{k+1} G_k)^{\top} \\
&+ \left[\overline{\gamma}(1 - \overline{\gamma})(1 + \varepsilon_k)\right] K_{k+1} G_k \Sigma_{k+1} G_k^{\top} K_{k+1}^{\top} \\
&+ \left[\left(1 - \overline{\gamma}^2\right)\varepsilon_k^{-1} \delta^2 + (1 - \overline{\gamma})\delta^2\right] K_{k+1} K_{k+1}^{\top} \\
&+ \overline{\gamma} K_{k+1} R K_{k+1}^{\top}.
\end{aligned} \tag{23}$$

Taking the partial derivation of the trace of the matrix Π_{k+1} with respect to $\mathbf{K}_{k+1}$ and letting the derivative be zero, we can obtain that

$$\begin{aligned}
&- 2\left[\overline{\gamma} + \left(\overline{\gamma} - \overline{\gamma}^2\right)\varepsilon_k\right] (I - \overline{\gamma} K_{k+1} G_k) P_{k+1|k} G_k^{\top} \\
&+ 2\overline{\gamma}(1 - \overline{\gamma})(1 + \varepsilon_k) K_{k+1} G_k \Sigma_{k+1} G_k^{\top} \\
&+ 2\left[\left(1 - \overline{\gamma}^2\right)\varepsilon_k^{-1} \delta^2 + (1 - \overline{\gamma})\delta^2\right] K_{k+1} \\
&+ 2\overline{\gamma} K_{k+1} R = 0.
\end{aligned} \tag{24}$$

It follows that

$$K_{k+1}\left[\alpha_1 G_k P_{k+1|k} G_k^{\top} + \alpha_2 G_k \Sigma_{k+1} G_k^{\top} + \alpha_3 I + R\right] = \alpha_4 P_{k+1|k} G_k^{\top}. \tag{25}$$

Since $\alpha_1 G_k P_{k+1|k} G_k^{\top} + \alpha_2 G_k \Sigma_{k+1} G_k^{\top} + \alpha_3 I + R$ is a positive definite matrix, we know (10) holds and the proof is complete. □

As we can see in equations (10) and (16), one needs $\mathcal{O}(n^3)$ operations to compute the Kalman gain and the covariance matrix $P_{k+1|k}$, where $n = 5$ in this paper. It indicates that the secure recursive estimator can be treated in a short time without a high-performance computer.

Remark 2. From (23), it can be seen that the larger δ leads to a bigger upper bound of the estimation error covariance, which means that the estimation performance deteriorates with increased δ.

Remark 3. According to the matrix inequality technique of Lemma 1, one can arbitrarily choose the positive constant ε_k in Theorem 1 from the theoretical point of view. However, a too large or too small value of ε_k may influence the estimation performance. In practice or experimental validation, we select the appropriate positive constant ε_k based on experience to achieve better estimation performance.

As a matter of fact, for autonomous vehicles in the presence of deception attacks (sensor attacks), how to obtain

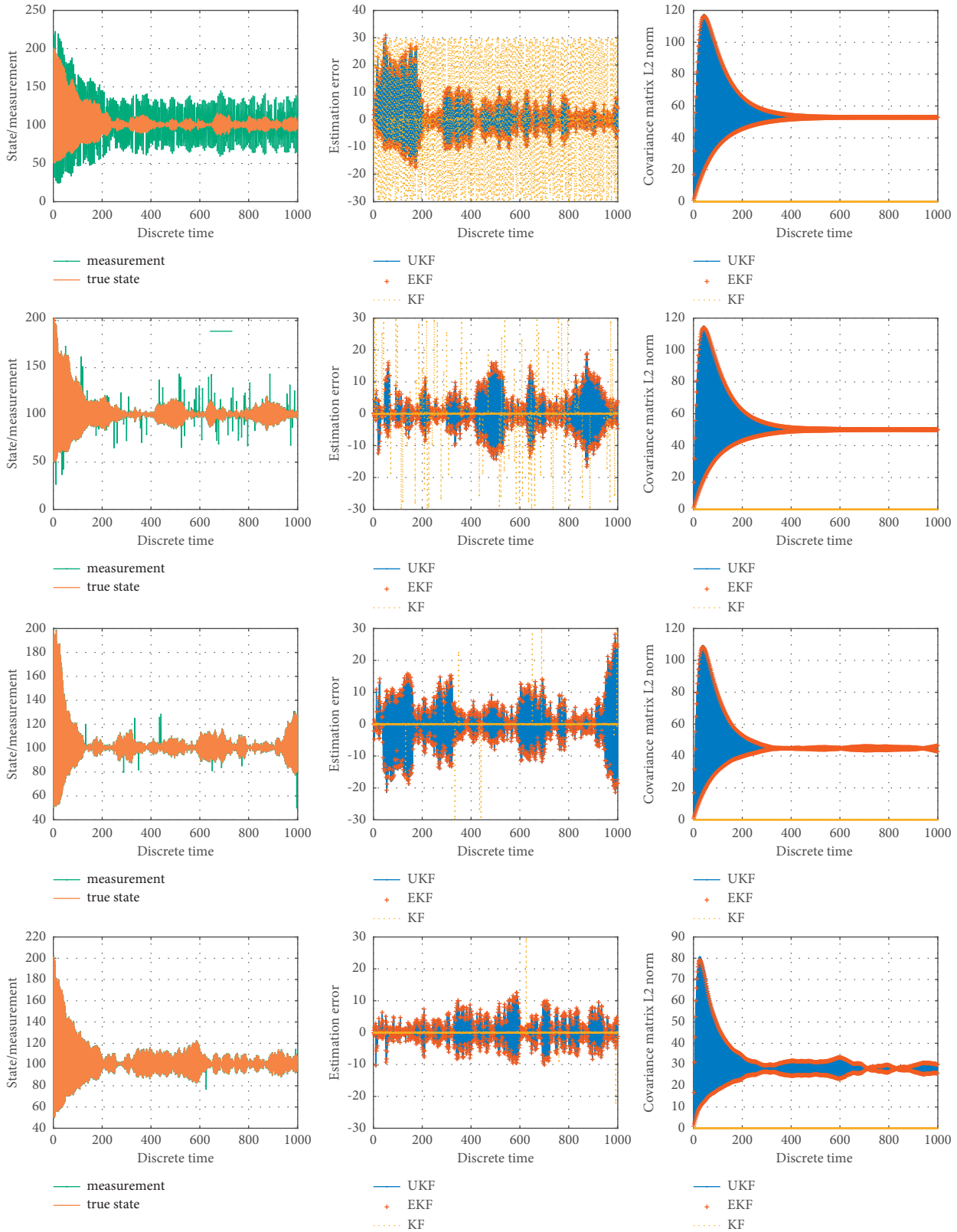

Figure 1: Simulation performance of the proposed filter (legend "UKF"), the filter in [18] (legend "EKF"), and the Kalman Filter (legend "KF"). The first column illustrates the ground truth state and measurement values. The second column shows estimation errors. The third column represents the norms of the estimator covariance matrices Π, which are real positive numbers in this case. The first to fourth rows show results where $\overline{\gamma} = 0.1$, 0.9, 0.99, and 0.999, respectively.

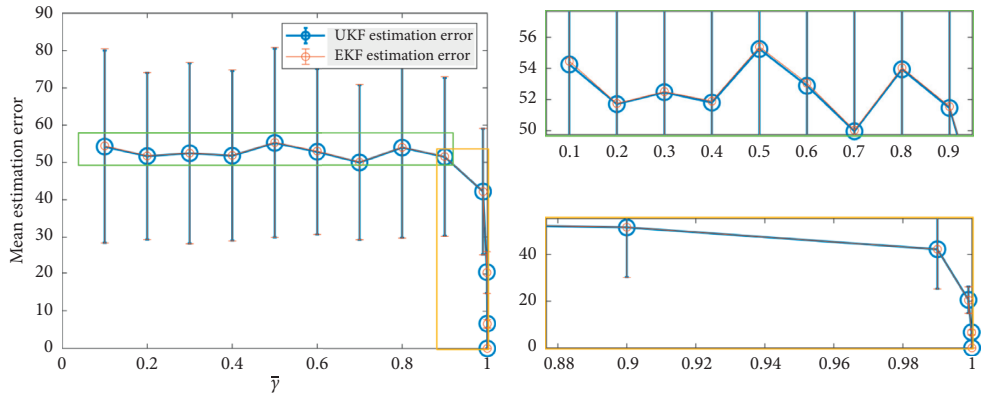

FIGURE 2: The estimation squared error bar graph with respect to $\overline{\gamma}$. The left figure represents the mean and standard deviation of squared errors under different nonattack probabilities in 500 simulations. The right figures show local details of the error graph. "UKF" and "EKF" denote the proposed filter and the approach in [18], respectively.

a secure pose estimation of discrete kinematic equation (1) remains an open problem till now. The goal of this paper is to propose an algorithm that enables to estimate the pose states of the autonomous vehicle in such a way that

(1) If no sensors are comprised, i.e., $\overline{\gamma} = 1$ and $\gamma_k = 0$ with probability 1 for all k, the estimate coincides with the standard Kalman filter

(2) If less than half of the pose states are compromised by randomly occurring deception attacks, it still gives a stable estimate of the pose states; i.e., an upper bound for the estimation error covariance is guaranteed

According to Theorem 1, the calculation framework can be summarized as in Algorithm 1.

5. Numeric Simulation

We first run the proposed approach based on a simple but effective Single-Input and Single-Output (SISO) system. Consider

$$x_{k+1} = \frac{10000}{x_k} + u_k + w_k,$$
$$z_k = x_k + v_k, \tag{26}$$

where the control $u_k = 1$ and the attack $a_k = 30$. The attack-related parameters are set as $\delta = 30$ and $\epsilon_k = 0.001$. The process and measurement noise levels are $Q = 1$ and $R = 0.01$, respectively. UKF parameters are $\alpha = 1e^{-3}$, $\kappa = 0$, and $\beta = 2$. The system is initialized as $x_0 = 50$.

We select this nonlinear process model and the identical measurement model because the proposed approach does not apply to nonlinear measurements directly. In other words, a linear approximation of measurement equation is always required, similar to [18]. The identical measurement equation allows direct comparison between the proposed approach and [18] and avoids unnecessary bias from measurement equation linearization. Although a simple model is used in simulation, experiments in the next section present algorithm performance based on a nonlinear measurement model.

Figure 1 shows the simulation performance under different attack intensities. Legends "UKF," "EKF," and "KF" denote the performance of the proposed approach, the method in [18], and the conventional Kalman filter. We select EKF and KF for comparison because these two methods are classical filters that have been widely used in practice. The comparison to classical methods gives readers a more intuitive illustration of the gain from the proposed approach. The first column illustrates the ground truth state and the measurement with attacks. As $\overline{\gamma}$ increases, the probability of attacks decreases, and the measurements are less interfered. The second column shows estimation error, where EKF and UKF result in similar and stable estimation errors that are less influenced by attack intensity $\overline{\gamma}$. The KF leads to large estimation error when $\overline{\gamma}$ is small but the estimation becomes much more accurate when there is a small chance of being attacked. However, as the KF does not consider the attack issue, estimation accuracy may deteriorate suddenly, at a discrete time around 620 with $\overline{\gamma} = 0.999$. The third column presents the norm of the estimator covariance matrix, which is a number in the SISO system. It is found that the KF gives a completely wrong estimation error covariance matrix by comparing the second and the third columns in Figure 1: KF outputs nearly zero estimation error covariance matrix, but the estimation errors are quite large under attacks. On the contrary, the proposed approach and [18] both provide reliable error upper bound covariance matrices.

To test the stability and robustness under random noises and attacks, we repeat the simulation 500 times and compute the error as $e = 1/N \sum_N \{(x - \hat{x})^2\}$ where N denotes the total number of discrete time indexes. The mean and standard deviation of error e with respect to nonattack probabilities are illustrated in Figure 2. From the results, it is noted that UKF performs slightly better than EKF for the simulated dynamic system. Moreover, both UKF and EKF estimation errors stay almost unchanged with $\overline{\gamma}$ from 0.1 to 0.9, but the errors drop dramatically with $\overline{\gamma}$ from 0.99 to 1.

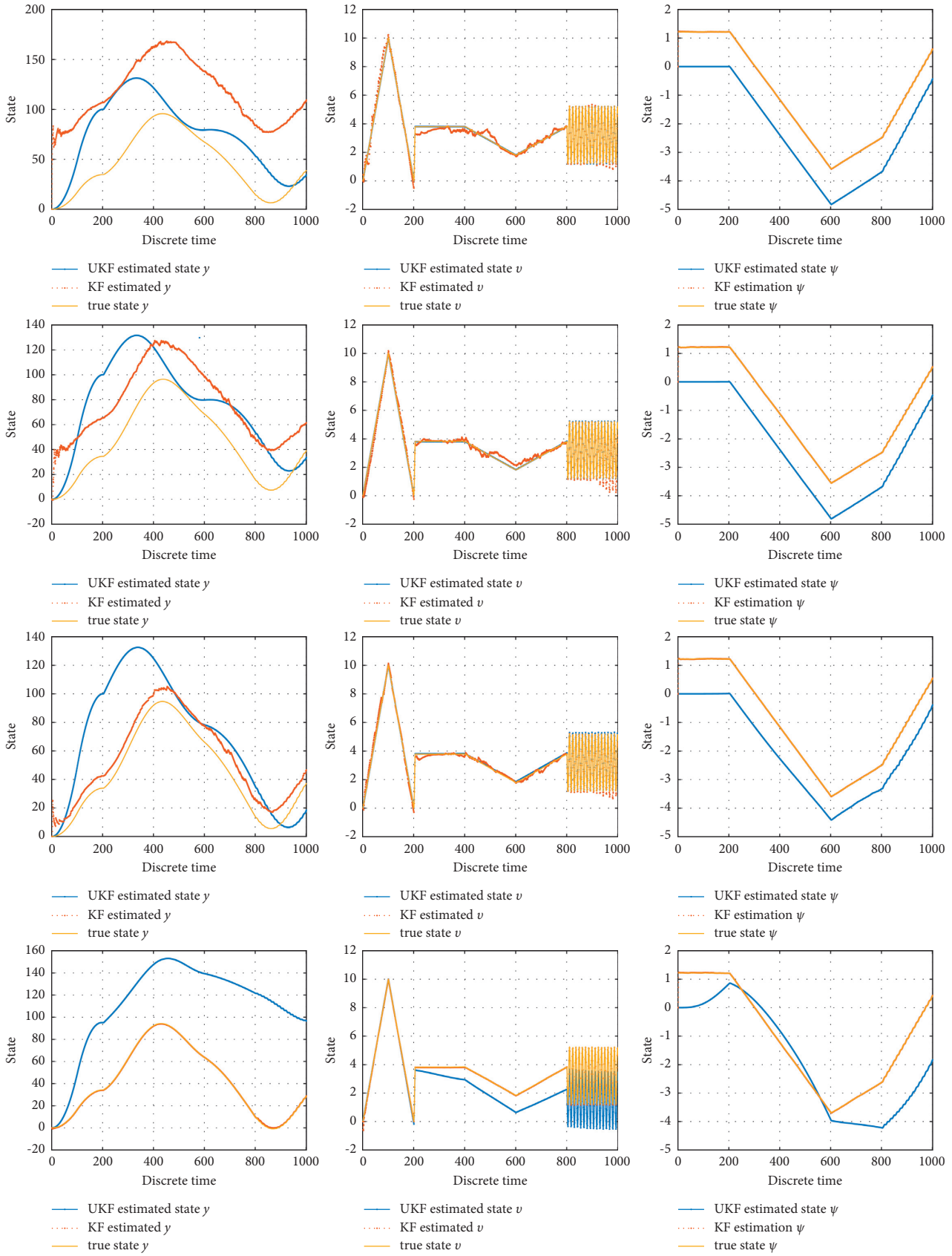

FIGURE 3: Pose estimation of selected states y (first column), v (second column), and ψ (third column) of the proposed filter (legend "UKF") and the Kalman filter (legend "KF"). The first to fourth rows show results where $\overline{\gamma}$ = 0.3, 0.7, 0.9, and 0.999, respectively.

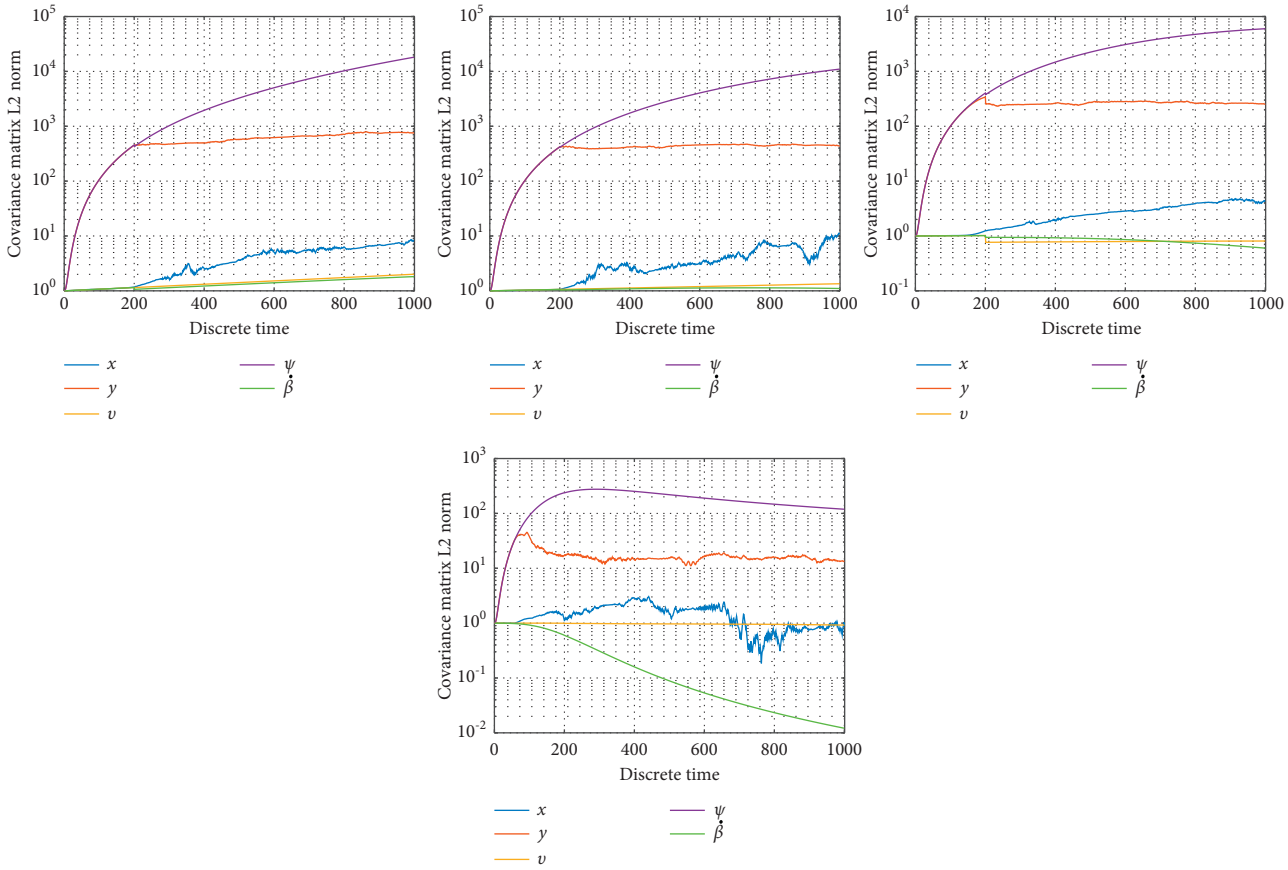

FIGURE 4: The diagonal elements in the estimation covariance matrices Π. The first to fourth rows show results where $\overline{\gamma} = 0.3$, 0.7, 0.9, and 0.999, respectively.

6. Experiments

We apply the proposed approach to the ground vehicle pose estimation problem that has been formulated in Section 3. The following attack signal is added to the measurement:

$$a_k = \begin{bmatrix} 10 & 10 & 0 & 0 & 0 \end{bmatrix}^\top. \tag{27}$$

The control signal reflects common driving behaviors and details can be found in our previous work [18]. The attack-related parameters are set as $\delta = 14$ and $\epsilon_k = 0.001$. The process and measurement noise levels are

$\mathbf{Q} = \text{diag}(0.001^2, 0.001^2, 0.001^2, 0.0005^2, 0.0001^2)$ and $\mathbf{R} = \text{diag}(1.0^2, 1.0^2, \texttt{deg2rad}^2(1), 0.5^2, \texttt{deg2rad}^2(2))$, respectively, where `deg2rad` denotes the conversion from degree to radian. UKF parameters are $\alpha = 1e^3$, $\kappa = 0$, and $\beta = 2$. The system is initialized as $\mathbf{x}_0 = [0, 0, 0.001, \texttt{deg2rad}(70), 0]^\top$.

In practice, the process and measurement noises of the filtering algorithms are unknown and need to be estimated using modeling or statistical approaches. In this paper, the process and measurement noises are identical to the ground truth, which is an optimal selection. All other shared parameters are kept the same for all the methods for a fair comparison.

6.1. General Performance. The pose estimation errors for selected states under different nonattack probabilities can be found in Figure 3. Note that we do not show EKF performance [18] in this section since EKF and UKF do not share the same parameters; thus, it is hard to compare these two methods fairly with different configurations. From the results, it is noted that the proposed estimation may perform worse when there is less attack, as shown in the last row of the figure, where $\overline{\gamma} = 0.999$ indicates that the chance of an attack is extremely low. In such case, the conventional Kalman filter performs well. If there are frequent attacks, the proposed estimator generally has more stable results than the Kalman filter with less sudden fluctuations. However, unlike the Kalman filter, the proposed approach does not guarantee the best linear estimation performance in the minimum mean-square-error sense, since we have only derived an upper bound of the estimation error covariance matrix. In this case, it is not a surprise to have poor estimation accuracy on some states, for example, y and ψ. The diagonal elements in the estimation error covariance matrices with respect to various nonattack probabilities ($\overline{\gamma} = 0.3, 0.7$, and 0.999) have been illustrated in Figure 4, where we could monitor the estimation quality on different states in real time. The results show that lower upper bounds are derived with larger $\overline{\gamma}$. Note that a larger $\overline{\gamma}$ does not ensure

a higher estimation accuracy but only gives a narrower range of estimation errors.

6.2. Influence of Parameters. It is observed during the experiments that the parameters of the estimator have a great influence on the performance. There are three configurable parameters in the proposed approach, namely δ, ϵ, and $\overline{\gamma}$. Theoretically, δ should be set according to the attacks. However, attack signal is unknown in practice and δ is set based on our experience and prediction of attacks. A conservative and large δ may lead to a large Π, while a small δ may get the violation of inequality (20) and invalidate the error covariance matrix Π. A large ϵ usually leads to divergence of the estimation; thus, it is set to a small value in all experiments. Finally, $\overline{\gamma}$ is set as the nonattack probability of attack signal. Practically $\overline{\gamma}$ is unknown and could be configured according to the threat level of attacks. Besides, UKF parameters influence the algorithm's performance. An appropriate selection of α, κ, and β is required to adjust the distribution of sigma points for the dynamic system. Still, tuning is necessary during experiments, since there is no direct guidance on UKF parameter selection.

7. Conclusion

In this work, a recursive pose estimator inspired by the unscented Kalman filter has been designed to tackle the secure vehicle pose estimation problem under random deception attacks. The estimator minimizes the upper bound of the estimation error covariance, which can be solved very efficiently in real time and is suitable for recursive computation in online applications. Simulations and experiments have been designed to validate the effectiveness of the proposed estimation approach. In the future, a particle filter-based estimator could be proposed for generalized dynamic systems.

Data Availability

The data used to support the findings of this study were supplied by the Xi'an University of Technology under license and so cannot be made freely available. Requests for access to these data should be made to Xinghua Liu.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partly supported by the National Natural Science Foundation of China under Grant 61903296 and U2003110, Innovative Talents Promotion Program Young Science and Technology Nova Project (2020KJXX-094), Key Laboratory Project of Shaanxi Educational Committee under Grant 20JS110, and High Level Plan of Shaanxi Province for Young Professionals.

References

[1] B. V. Philip, T. Alpcan, J. Jin, and M. Palaniswami, "Distributed real-time iot for autonomous vehicles," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 2, pp. 1131–1140, 2018.

[2] C. Urmson and W. Whittaker, "Self-driving cars and the urban challenge," *IEEE Intelligent Systems*, vol. 23, no. 2, pp. 66–68, 2008.

[3] J. Guo, R. Jiang, B. He, T. Yan, and S. S. Ge, "General learning modeling for auv position tracking," *IEEE Intelligent Systems*, vol. 35, 2020.

[4] M. Strohmeier, T. Walter, J. Rothe, and S. Montenegro, "Ultra-wideband based pose estimation for small unmanned aerial vehicles," *IEEE Access*, vol. 6, pp. 57526–57535, 2018.

[5] R. Jiang, H. Zhou, H. Wang, and S. S. Ge, "Road-constrained geometric pose estimation for ground vehicles," *IEEE Transactions on Automation Science and Engineering*, vol. 17, no. 2, pp. 748–760, 2020.

[6] Q. Liu, Y. Mo, X. Mo, C. Lv, E. Mihankhah, and D. Wang, "Secure pose estimation for autonomous vehicles under cyber attacks," in *Proceedings of the 2019 IEEE Intelligent Vehicles Symposium (IV)*, pp. 1583–1588, IEEE, Paris, France, June 2019.

[7] L. Shi, Q. Liu, J. Shao, and Y. Cheng, "Distributed localization in wireless sensor networks under denial-of-service attacks," *IEEE Control Systems Letters*, vol. 5, no. 2, pp. 493–498, 2021.

[8] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 5, pp. 779–789, 2018.

[9] C. Meng and W. Li, "Recursive filtering for complex networks against random deception attacks," in *Proceedings of the 2018 IEEE International Conference on Big Data and Smart Computing (BigComp)*, pp. 565–568, IEEE, Shanghai, China, January 2018.

[10] Z. Ju, H. Zhang, and Y. Tan, "Deception attack detection and estimation for a local vehicle in vehicle platooning based on a modified ufir estimator," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 3693–3705, 2020.

[11] 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.

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

[13] S. Mishra, Y. Shoukry, N. Karamchandani, S. N. Diggavi, and P. Tabuada, "Secure state estimation against sensor attacks in the presence of noise," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 49–59, 2017.

[14] L. Liu, H. Li, Y. Dai, and Q. Pan, "Robust and efficient relative pose with a multi-camera system for autonomous driving in highly dynamic environments," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2432–2444, 2018.

[15] X. Ding, Z. Wang, L. Zhang, and C. Wang, "Longitudinal vehicle speed estimation for four-wheel-independently-actuated electric vehicles based on multi-sensor fusion," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 11, pp. 12797–12806, 2020.

[16] 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.

[17] C. Wang, Z. Wang, L. Zhang, D. Cao, and D. G. Dorrell, "A vehicle rollover evaluation system based on enabling state and parameter estimation," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4003–4013, 2021.

[18] X. Liu, R. Jiang, H. Wang, and S. S. Ge, "Filter-based secure dynamic pose estimation for autonomous vehicles," *IEEE Sensors Journal*, vol. 19, no. 15, pp. 6298–6308, 2019.

[19] A. Kelly, *Mobile Robotics: Mathematics, Models, and Methods*, Cambridge University Press, Cambridge, UK, 2013.

[20] B. Shen, Z. Wang, D. Wang, and Q. Li, "State-saturated recursive filter design for stochastic time-varying nonlinear complex networks under deception attacks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 31, no. 10, pp. 3788–3800, 2020.

[21] W.-H. Chen and W. X. Zheng, "Delay-dependent robust stabilization for uncertain neutral systems with distributed delays," *Automatica*, vol. 43, no. 1, pp. 95–104, 2007.