

Sparsity-Aware Sensor Selection for Privacy-Preserving Zonotopic Fusion Filtering in Cloud-Based Vehicle Tracking Systems

Kaiqun Zhu, Zidong Wang, Xinhua Zheng, Zhenning Li and Keqiang Li

Abstract—This paper investigates the zonotopic filtering problem for cloud-based vehicle tracking systems under joint privacy and communication bandwidth constraints. Cloud-side tracking platforms improve vehicle state estimation accuracy by fusing multi-source measurements collected from roadside nodes. However, during roadside-to-cloud data transmission, the system is confronted with coupled challenges arising from privacy leakage risks and the communication burden induced by concurrent data uploads from large-scale sensor deployments. To address these challenges, a zonotopic fusion filtering framework incorporating privacy-preserving mechanisms and sparsity-aware sensor selection strategies is proposed to achieve a balanced trade-off among privacy protection, communication efficiency, and estimation accuracy. First, a novel secret-sharing-based zonotopic fusion filtering method is developed, which embeds a dynamic-encoding-based secret sharing mechanism into the multi-sensor fusion process to protect both transmitted data and estimation results. Furthermore, to reduce redundant communications, a sparsity-promoting sensor selection scheme is constructed by introducing a sparsity penalty into the filter parameter optimization problem, enabling transmission only from sensors that effectively contribute to the current estimation accuracy. The resulting optimization problem is solved using convex relaxation and the alternating direction method of multipliers, yielding analytical update expressions for the filter parameters. In addition, the boundedness of the vehicle state estimation error is rigorously analyzed, and a sufficient condition ensuring that the estimation error remains bounded is established. Finally, simulation experiments demonstrate the effectiveness of the proposed algorithm in achieving accurate, communication-efficient, and privacy-

preserving state estimation.

Index Terms—Cloud-based vehicle tracking, zonotopic fusion filtering, privacy preservation, secret sharing mechanism, sensor selection, communication constraints.

I. INTRODUCTION

With the rapid development of autonomous driving and intelligent transportation systems, vehicle-road-cloud collaboration has emerged as a key technological paradigm to enhance traffic safety, operational efficiency, and global perception capability [8]. Within this architecture, the cloud platform relies on multi-source information uploaded by roadside sensing nodes to perform remote perception and dynamic tracking of vehicle states, thereby supporting tasks such as trajectory prediction, traffic scheduling, and risk warning. However, the continuous uploading of multi-sensor data, although improving the cloud-side perception accuracy, also imposes a substantial communication burden [18], [21], [32], [37]. Furthermore, vehicle information such as position and velocity is highly sensitive, and once eavesdropped or maliciously exploited during transmission, such information may lead to privacy leakage, compromised decision-making in the cloud, and even traffic safety threats [1], [19], [31], [34]. Therefore, achieving a balance among estimation accuracy, communication efficiency, and privacy preservation has become a critical challenge in vehicle tracking for vehicle-road-cloud systems.

From the perspective of state estimation, classical stochastic filtering methods typically rely on precise prior knowledge of noise statistics [5], [17]. In real traffic environments, however, process disturbances, measurement noise, and communication-induced uncertainties are often difficult to model accurately; such uncertainties are typically characterized as unknown in probability distribution but bounded in magnitude [3], [9], [20], [35], [40]. In contrast, the zonotopic filtering method describes the bounded region of estimation error through set recursion and thus provides guaranteed state envelopes under unknown bounded disturbances, making it suitable for robust estimation in complex transportation systems [2], [39]. Although substantial progress has been made in multi-sensor fusion and set-membership estimation (see e.g., [13], [30], [33]), most existing methods are primarily designed for scenarios where all sensors fully participate and transmit plaintext data, which limits their applicability in vehicle-road-cloud systems subject to communication and privacy constraints.

In recent years, privacy preservation has become an important research focus in state estimation and control [7],

This work was supported in part by the Science and Technology Development Fund of Macau under Grant 0007/2025/RIC, Grant 0122/2024/RIB2, Grant 0215/2024/AGJ, Grant 0074/2025/AMJ, Grant 001/2024/SKL, and Grant 0002/2025/EQP; in part by the Research Services and Knowledge Transfer Office of University of Macau under Grant SRG2023-00037-IOTSC and Grant MYRG-GRG2024-00284-IOTSC; in part by the Shenzhen-Hong Kong-Macau Science and Technology Program Category C under Grant SGD20230821095159012; in part by the Science and Technology Planning Project of Guangdong under Grant 2025A0505010016; in part by the National Natural Science Foundation of China under Grant 52572354; in part by the State Key Lab of Intelligent Transportation System under Grant 2024-B001; in part by the Jiangsu Provincial Science and Technology Program under Grant BZ2024055; in part by the Royal Society of the UK; and in part by the Alexander von Humboldt Foundation of Germany. (Corresponding author: Zhenning Li.)

Kaiqun Zhu and Zhenning Li are with the State Key Laboratory of Internet of Things for Smart City, University of Macau, Macau 999078, China. (Email: kaiqunzhu@um.edu.mo; zhenningli@um.edu.mo)

Zidong Wang is with the Department of Computer Science, Brunel University of London, Uxbridge, Middlesex, UB8 3PH, United Kingdom. (Email: Zidong.Wang@brunel.ac.uk)

Xinhua Zheng is with the Intelligent Transportation Thrust, Systems Hub, The Hong Kong University of Science and Technology (Guangzhou), Guangzhou 511455, China. (Email: xinhuzheng@hkust-gz.edu.cn)

Keqiang Li is with the School of Vehicle and Mobility, Tsinghua University, Beijing 100084, China. (Email: likq@tsinghua.edu.cn)

[16], [36]. Existing studies have shown that incorporating privacy-preserving mechanisms into dynamic systems is both necessary and feasible [10], [11], [22], [28], [38]. Among the representative approaches, the homomorphic encryption technique enables computation over ciphertexts but is computationally intensive and thus unsuitable for resource-constrained roadside sensors. The differential privacy mechanism offers computational efficiency but inevitably introduces additional noise, degrading estimation accuracy. By contrast, the secret sharing approach achieves information-theoretic security with lightweight computation and inherent fault tolerance, making it a promising solution for privacy preservation in vehicle-road-cloud systems. Nevertheless, the secret sharing scheme also introduces new challenges: since transmitted data must be compatible with finite-field operations, real-valued measurements require dynamic encoding, integer mapping, and decoding, which inevitably introduce additional distortion. This distortion may be further coupled with measurement noise, external disturbances, and filtering errors, thereby increasing the difficulty of estimator design and performance analysis.

In cloud-based multi-sensor tracking systems, not all sensors contribute equally to estimation accuracy at every time instant. If all roadside nodes continuously upload their data in full, such a strategy may, under ideal conditions, enrich the information available for fusion. However, in vehicle-road-cloud environments with limited communication resources, full data transmission can substantially increase the network burden and may lead to data congestion, increased transmission delays, and incomplete measurement information, thereby degrading the cloud-based state estimation and control performance [23], [26], [27], [29]. Consequently, adaptively selecting a small subset of key sensors that contribute most to estimation accuracy presents an effective strategy for improving communication efficiency while maintaining acceptable estimation performance [6], [24]. However, the sensor selection problem is often formulated as a non-convex optimization with cardinality constraints. When coupled with the distortion induced by secret sharing schemes and the recursive zonotopic filtering process, the overall problem becomes considerably more complex. In other words, the core challenge and practical significance of this study lie in achieving sparse sensor selection under privacy-preserving constraints while simultaneously ensuring the estimation accuracy of vehicle states and the boundedness of estimation errors.

In recent years, research on vehicle state estimation algorithms in vehicle-road-cloud systems has made considerable progress. However, several critical issues remain to be addressed. First, full sensor participation may incur unnecessary communication and computational overhead, thereby limiting the scalability of cloud-based vehicle tracking systems in large-scale scenarios. Second, plaintext data transmission may lead to the disclosure of vehicle state information and weaken the privacy-preserving capability of the system. In addition, the lack of explicit communication constraints may hinder the deployment of estimation algorithms in practical environments with limited bandwidth and transmission resources. These issues may further degrade cloud-side estimation accuracy, impair the reliability of cloud-based decision-making, and

even pose potential traffic safety risks.

Motivated by these observations, how to develop a state estimation algorithm within the zonotopic filtering framework by jointly incorporating secret-sharing mechanisms and sensor selection strategies constitutes a theoretically significant and practically valuable challenge. Furthermore, how to systematically characterize the coupling among state estimation performance, the secret-sharing mechanism, and the sensor selection strategy, how to explicitly construct a sensor selection strategy based on estimation performance indices, and how to establish the boundedness analysis of the estimation error remain key problems that deserve further investigation.

This paper investigates the privacy-preserving zonotopic fusion filtering problem under a sparse sensing strategy for cloud-based vehicle tracking systems. The main contributions are summarized as follows.

- 1) *A novel secret-sharing-based zonotopic fusion filtering framework is proposed.* By embedding a dynamic encoding-based secret sharing mechanism into the fusion filtering process, the proposed framework alleviates the communication burden and protects vehicle information privacy during data transmission, while ensuring the accuracy of the resulting state estimates.
- 2) *A sparsity-aware optimization scheme for filter parameter design is developed.* By incorporating sparsity constraints into the filter gain design, the proposed scheme can identify sensor nodes that are informative for the current state estimation, thereby reducing redundant data transmission. In addition, by employing group-lasso-based convex relaxation and the alternating direction method of multipliers, computationally tractable analytical update expressions are derived, and a corresponding sensor selection strategy is obtained, achieving an effective balance between communication cost and estimation accuracy.
- 3) *A rigorous boundedness analysis of the vehicle-state estimation error is provided.* The effects of both the distortion introduced by the secret sharing mechanism and the sparse filter structure induced by the sparsity-aware design are explicitly taken into account. Based on this, sufficient conditions are established to guarantee bounded estimation errors, thereby ensuring the reliability and stability of the proposed method under privacy-preserving and sparse-transmission constraints.

Notations: $\|\cdot\|_1$, $\|\cdot\|_2$, $\|\cdot\|_\infty$, $\|\cdot\|_F$ denote, respectively, the 1-norm, 2-norm, the ∞ -norm, and the Frobenius norm; $\{a_i\}_{i=1}^n \triangleq \{a_1, a_2, \dots, a_n\}$; $\text{diag}\{M_1, M_2, \dots, M_n\}$ is a block-diagonal matrix with n blocks; and $\text{Tr}(M)$ is the trace of a matrix M .

II. PROBLEM FORMULATION

In the considered vehicle-road-cloud system, the cloud platform estimates vehicle states from measurements collected by multiple roadside sensing nodes. To enable privacy-preserving and communication-efficient tracking, a secret-sharing mechanism together with a sparsity-aware sensor selection strategy is integrated into the framework. This section first presents

the system model and then formulates the corresponding zonotopic filtering problem under the proposed secret-sharing mechanism and sensor selection strategy

To facilitate the presentation of the problem, we first provide the following definitions and lemmas related to the zonotopic filtering algorithm.

Definition 1: [12] An l -order zonotope is given by

$$\langle c, G \rangle \triangleq \{z \mid z = c + G\beta, \|\beta\|_\infty \leq 1\}$$

where $c \in \mathbb{R}^n$ and $G \in \mathbb{R}^{n \times l}$ are the center and the generator matrix of the zonotope, respectively.

Lemma 1: [12] Given two zonotopes $\langle c_1, G_1 \rangle$ and $\langle c_2, G_2 \rangle$, one has

$$\langle c_1, G_1 \rangle \oplus \langle c_2, G_2 \rangle = \langle c_1 + c_2, [G_1 \ G_2] \rangle \quad (1)$$

$$\mathcal{S}\langle c_1, G_1 \rangle = \langle \mathcal{S}c_1, \mathcal{S}G_1 \rangle \quad (2)$$

$$\langle c_1, G_1 \rangle \subseteq \langle c_1, \mathbf{rs}(G_1) \rangle \quad (3)$$

where $\oplus$ is the Minkowski sum, $\mathcal{S}$ is the scaling matrix, and

$$\mathbf{rs}(G_1) \triangleq \text{diag}\{\|G_{1,1}\|_1, \|G_{1,2}\|_1, \dots, \|G_{1,n}\|_1\}$$

with $G_{1,m}$ being the m -th row vector of the matrix G_1 .

A. Vehicle Model

This paper adopts the following discrete-time model to characterize the vehicle tracking process in typical urban-road or highway scenarios where the vehicle motion is locally smooth over short sampling intervals, such as cruising at an approximately constant velocity or mild acceleration/deceleration. The model captures the position and velocity information of the vehicle in both the longitudinal and lateral directions:

$$x_{k+1} = Ax_k + Bw_k \quad (4)$$

with

$$x_k = \begin{bmatrix} p_{x,k} \\ p_{y,k} \\ v_{x,k} \\ v_{y,k} \end{bmatrix}, \quad A = \begin{bmatrix} 1 & 0 & \delta & 0 \\ 0 & 1 & 0 & \delta \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} \frac{\delta^2}{2} & 0 \\ 0 & \frac{\delta^2}{2} \\ \delta & 0 \\ 0 & \delta \end{bmatrix}.$$

Here, $p_{x,k}$, $p_{y,k}$, $v_{x,k}$, and $v_{y,k}$ are, respectively, the positions and speeds along the x -axis and y -axis; δ is the sampling period; and w_k denotes the disturbance input satisfying

$$w_k \in \langle 0, Q_k \rangle \quad (5)$$

with Q_k being the known matrix. Here, w_k can be interpreted as the unmodeled acceleration/deceleration components along the two axes.

In a vehicle-road-cloud cooperation system, the vehicle states are measured by sensors deployed along the roadside infrastructure. The measurement obtained by the i -th sensor is

$$y_{i,k} = C_i x_k + v_{i,k}, \quad i = 1, 2, \dots, M \quad (6)$$

where $y_{i,k}$ is the measurement signal, C_i is the measurement matrix, and $v_{i,k}$ is the measurement noise satisfying

$$v_{i,k} \in \langle 0, R_{i,k} \rangle \quad (7)$$

with $R_{i,k}$ being the known matrix.

B. Privacy-Preserving Mechanism

In an intelligent vehicle-road-cloud system, roadside sensors are required to transmit the collected traffic data to the cloud through the network for further analysis and processing. However, such information is susceptible to interception by eavesdroppers during transmission. Adversaries may exploit the recovered data to launch malicious cyberattacks, thereby compromising the accuracy of cloud-side information processing and posing potential threats to road traffic safety. To ensure secure data transmission, this section proposes a dynamic-encoding-based secret sharing mechanism.

The secret sharing mechanism consists of two main steps: secret distribution (i.e., encryption) and secret reconstruction (i.e., decryption) [25]. In the secret distribution phase, the roadside sensors employ an encryption function (8) to generate n shares of secret data, denoted as $\text{Enc}(S, z_\iota)$, where $\iota = 1, 2, \dots, n$. During the secret reconstruction phase, the cloud platform can recover the original plaintext information using any t ($2 \leq t \leq n$) of these secret shares with the aid of the decryption function (10). The detailed procedure is presented in Algorithm 1.

Algorithm 1 The (t, n) -Threshold Secret Sharing Scheme

Input: Secret $S \in \mathbb{F}_p$, threshold t , number of participants n

Output: n shares, where any t shares can reconstruct S

- 1: Select a large prime p and define a finite field $\mathbb{F}_p$ with $\mathbb{F}_p \triangleq \{0, 1, 2, \dots, p-1\}$
- 2: Randomly choose coefficients: $a_1, a_2, \dots, a_{t-1} \in \mathbb{F}_p$
- 3: Construct the polynomial encryption function:

$$\text{Enc}(S, z) = S + \sum_{j=1}^{t-1} a_j z^j \pmod{p} \quad (8)$$

4: **procedure** SECRET DISTRIBUTION (ENCRYPTION)

5: **for** $\iota \leftarrow 1$ to n **do**

6: Compute a share $s_{z_\iota} = \text{Enc}(S, z_\iota)$

7: Send s_{z_ι} to the cloud platform

8: **end for**

9: **end procedure**

10: **procedure** SECRET RECONSTRUCTION (DECRYPTION)

11: **for** $j \leftarrow 1$ to t **do**

12: Compute Lagrange coefficients:

$$\lambda_j = \prod_{\substack{m=1 \\ m \neq j}}^t \frac{z_m}{z_m - z_j} \pmod{p} \quad (9)$$

13: **end for**

14: Recover the secret using the decryption function:

$$S = \text{Dec}(\{s_{z_j}\}_{j=1}^t) = \sum_{j=1}^t s_{z_j} \cdot \lambda_j \pmod{p} \quad (10)$$

15: **return** S

16: **end procedure**

According to the encryption principle of the secret sharing mechanism, the plaintext to be encrypted must be an integer. However, vehicle information measured by roadside sensors is typically non-integer. Therefore, an integerization process is required prior to encryption. To alleviate the communication

burden, this paper introduces an integerization scheme based on a dynamic encoding mechanism that reduces the bits required for integer representation. The specific scheme is described as follows.

The dynamic-encoding-based integerization rule for the ℓ -th component of the sensor-measured information (e.g., $y_{i,k}$) is described as

$$\text{Int}(y_{i,k}^{[\ell]}) = \left\lceil \frac{2^{b_{i,k}-1}}{r\beta_i} (y_{i,k}^{[\ell]} - \alpha_i \chi_{i,k-1}^{[\ell]}) \right\rceil + 2^{b_{i,k}-1} - 1 \quad (11)$$

where $\lceil \cdot \rceil$ denotes the ceiling function that rounds a real number upward to the nearest integer and

$$\chi_{i,k}^{[\ell]} = \alpha_i \chi_{i,k-1}^{[\ell]} + \frac{r\beta_i}{2^{b_{i,k}-1}} \left\lceil \frac{2^{b_{i,k}-1}}{r\beta_i} (y_{i,k}^{[\ell]} - \alpha_i \chi_{i,k-1}^{[\ell]}) \right\rceil \quad (12)$$

with $b_{i,k}$ being the bit-width used for integerization, $r > 0$ being the clipping bound, and $\alpha_i > 0$ and $\beta_i > 0$ being known parameters. Then, according to (8) and (11), the dynamic-encoding-based encryption rule is given as $\text{Enc}(\text{Int}(y_{i,k}^{[\ell]}), z_i)$.

On the cloud platform, the decryption process is first carried out using t shares to reconstruct the encrypted data. Subsequently, the dynamic decoding rule is applied to recover the measurement information:

$$\begin{aligned} \llbracket y_{i,k}^{[\ell]} \rrbracket &= \alpha_i \llbracket y_{i,k-1}^{[\ell]} \rrbracket + \frac{r\beta_i}{2^{b_{i,k}-1}} (\text{Dec}(\{\mathcal{Y}_j\}_{j=1}^t) \\ &\quad - 2^{b_{i,k}-1} + 1) \end{aligned} \quad (13)$$

where $\llbracket y_{i,k}^{[\ell]} \rrbracket$ means the amplitude-discretized measurement information, $\llbracket y_{i,0}^{[\ell]} \rrbracket = \chi_{i,0}^{[\ell]}$, and $\mathcal{Y}_j \triangleq \text{Enc}(\text{Int}(y_{i,k}^{[\ell]}), z_j)$.

Based on (11)–(13), the encryption and decryption rule for the vector case is given as

$$\llbracket y_{i,k} \rrbracket = \begin{bmatrix} \llbracket y_{i,k}^{[1]} \rrbracket & \llbracket y_{i,k}^{[2]} \rrbracket & \cdots & \llbracket y_{i,k}^{[n_y]} \rrbracket \end{bmatrix}^T. \quad (14)$$

Remark 1: In practical engineering applications, the selection of the parameters r , α_i , β_i , and $b_{i,k}$ is closely related to the filtering performance. Specifically, r should be determined according to the variation range of the variable to be encoded, so as to ensure that the encoded variable remains within the prescribed effective encoding interval. Then, β_i can be selected according to the specific network communication conditions. For instance, when communication resources are limited, β_i may be appropriately increased to reduce the communication burden. On this basis, α_i can be further tuned empirically. When r , α_i , and β_i are fixed, a larger number of bits $b_{i,k}$ leads to a smaller decoding error and thus a weaker adverse effect on the filtering performance. In practical applications, for each component, when the ratio between the magnitude of the decoding error and that of the measurement noise is less than 0.1, the influence of the decoding error on the filtering performance is generally minor. In this case, further increasing the number of bits brings only limited improvement in filtering performance. Therefore, $b_{i,k}$ can be selected with reference to the condition $b_{i,k} \geq \log_2 \left(\frac{10r\beta_i}{\bar{v}_i^{[\ell]}} \right)$. Here, $\bar{v}_i^{[\ell]}$ denotes the upper bound on the absolute value of the ℓ -th component of the measurement noise $v_{i,k}$.

Remark 2: To address eavesdropping attacks during communication, the dynamic-encoding-based secret sharing mechanism constructed in this paper achieves information-theoretic security that is independent of the adversary's computational capability. Specifically, when the number of valid shares intercepted by an adversary is smaller than the threshold t , the plaintext information cannot be inferred from the obtained shares, regardless of the adversary's computational power. In addition, compared with privacy-preserving methods such as differential privacy technique and homomorphic encryption technique, the proposed method offers the additional advantage of stronger robustness.

C. Privacy-Preserving Zonotopic Filter

Based on the measurement information from roadside sensors, a zonotopic centralized fusion filter structure incorporating a secret sharing mechanism is designed, as shown below.

$$\vec{x}_{k+1} = A\hat{x}_k \quad (15)$$

$$\hat{x}_{k+1} = \vec{x}_{k+1} + K_{k+1}(\llbracket y_{k+1} \rrbracket - C\vec{x}_{k+1}) \quad (16)$$

where $\vec{x}_k$ is the one-step prediction, $\hat{x}_k$ means the estimated state, K_k is the filter parameter, and

$$\begin{aligned} \llbracket y_k \rrbracket &\triangleq \begin{bmatrix} \llbracket y_{1,k} \rrbracket & \llbracket y_{2,k} \rrbracket & \cdots & \llbracket y_{M,k} \rrbracket \end{bmatrix}^T \\ C &\triangleq \begin{bmatrix} C_1^T & C_2^T & \cdots & C_M^T \end{bmatrix}^T. \end{aligned}$$

Then, by denoting $\vec{e}_k \triangleq x_k - \vec{x}_k$ and $e_k \triangleq x_k - \hat{x}_k$, and by using (4) together with (15)–(16), one has

$$\vec{e}_{k+1} = Ae_k + Bw_k \quad (17)$$

$$e_{k+1} = (I - K_{k+1}C)\vec{e}_{k+1} - K_{k+1}(v_{k+1} + \delta_{k+1}) \quad (18)$$

where $\delta_k \triangleq \llbracket y_k \rrbracket - y_k$ and $v_k \triangleq [v_{1,k}^T \ v_{2,k}^T \ \cdots \ v_{M,k}^T]^T$.

The fundamental concept of zonotopic filtering [2], [14] is to design the filter such that the estimation error e_{k+1} remains constrained within a zonotope set (i.e., $e_{k+1} \in \langle 0, P_{k+1} \rangle$), where P_{k+1} denotes the generator matrix. This matrix variable P_{k+1} is closely related to both the estimation error and the filter gain, serving as a critical indicator of filtering accuracy. Therefore, within the zonotopic filtering framework, the filter parameters are determined by solving the following optimization problem:

$$\min_{K_{k+1}} \text{Tr}(P_{k+1}P_{k+1}^T). \quad (19)$$

In vehicle-road-cloud collaboration systems, roadside sensors transmit measurement data to the cloud via communication networks to achieve accurate vehicle state estimation. However, since network resources are usually limited, connecting an excessive number of sensors will significantly increase the communication burden, which may degrade the integrity of measurement signals. As a result, state estimation based on such incomplete measurements tends to suffer from deteriorated estimation performance.

To tackle this problem, it is necessary to reduce data transmissions from sensors as much as possible while guaranteeing acceptable estimation accuracy, so as to strike a balance

between estimation performance and communication resource utilization. In the state estimation system (16), the block matrix

$$K_{k+1} = [K_{1,k+1} \quad K_{2,k+1} \quad \cdots \quad K_{M,k+1}] \quad (20)$$

is partitioned into M block columns, where $K_{i,k+1}$ denotes the block column associated with the i -th sensor. Motivated by this observation, sparsity constraints can be imposed on the filter parameters such that sensors contributing more substantially to estimation accuracy are prioritized for data transmission. Accordingly, an optimization problem is formulated in this study, whose performance index incorporates both estimation accuracy and a sparsity penalty term, aiming to jointly determine the filter parameters and sensor selection strategy, which is expressed as follows:

$$\min_{K_{k+1}} \text{Tr}(P_{k+1} P_{k+1}^T) + \gamma J(K_{k+1}) \quad (21)$$

where $\gamma > 0$ is the weight parameter and $J(K_k)$ is the sparsity penalty function with

$$J(K_k) \triangleq \text{card}(\{ \|K_{1,k}\|_2 \quad \|K_{2,k}\|_2 \quad \cdots \quad \|K_{M,k}\|_2 \}). \quad (22)$$

Here, $\text{card}(\vartheta)$ is the cardinality function, which represents the number of nonzero components of a vector ϑ .

This paper aims to develop a zonotopic fusion filtering framework with sparsity awareness and privacy-preserving capabilities for cloud-based vehicle tracking systems, enabling high-precision and secure state estimation of vehicles, see Fig. 1. The main research objectives include:

- 1) solving the optimization problem (21) with the sparsity penalty function to obtain sparsity-promoting filter parameters; and
- 2) investigating the integrated influence of the secret sharing scheme and sparsity constraints on the filtering process, and analyzing the stability performance of the estimation error.

III. SPARSITY-AWARE SECRET-SHARING-BASED ZONOTOPIC FUSION FILTERING

In this section, we analyze the optimization problem (21) and propose a method for obtaining the sparsity-promoting filter parameters.

Before proceeding with the subsequent analysis, the following necessary lemmas are introduced.

Lemma 2: Considering the dynamic-encoding-based secret sharing scheme (11)–(13), one has

$$\delta_k \in \langle 0, \Delta_k \rangle \quad (23)$$

where $\delta_k \triangleq \llbracket y_k \rrbracket - y_k$ means the distorted data and

$$\Delta_k \triangleq \text{diag} \left\{ \frac{r\beta_1}{2^{b_{1,k}-1}} I, \frac{r\beta_2}{2^{b_{2,k}-1}} I, \dots, \frac{r\beta_M}{2^{b_{M,k}-1}} I \right\}.$$

Proof: See Appendix A. ■

Lemma 3: Given the initial condition $e_0 \in \langle 0, P_0 \rangle$, if $e_k \in \langle 0, P_k \rangle$, then $e_{k+1} \in \langle 0, P_{k+1} \rangle$, where the generator matrix P_{k+1} is computed according to

$$P_{k+1} = [\vec{K}_{k+1} \Psi_{k+1} \quad -K_{k+1} R_{k+1} \quad -K_{k+1} \Delta_{k+1}] \quad (24)$$

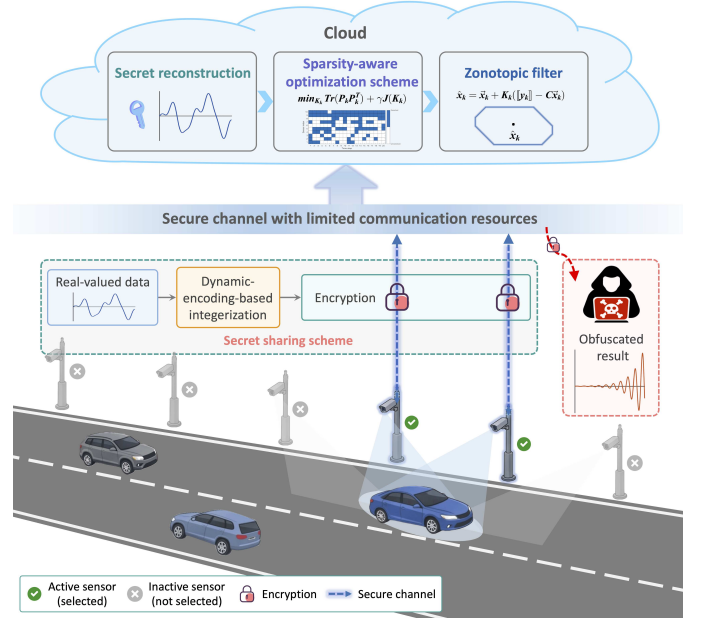


Fig. 1: The privacy-preserving zonotopic fusion filtering framework under sparsity-aware strategies.

$$\Psi_{k+1} = [AP_k \quad BQ_k] \quad (25)$$

with

$$\begin{aligned} \vec{K}_k &\triangleq I - K_k C \\ R_k &\triangleq \text{diag}\{R_{1,k}, R_{2,k}, \dots, R_{M,k}\}. \end{aligned}$$

Proof: See Appendix B. ■

Lemmas 2–3 establish the analytical structure of the generator matrices for zonotopes bounding the data distortion δ_k , prediction error $\vec{e}_k$, and estimation error e_k , forming the basis for the subsequent derivation of filter parameters.

Next, this section presents a detailed analysis of optimization problem (21) and develops an approach for solving it. Since the sparsity regularization term $J(K_k)$ in (21) involves the non-convex cardinality function $\text{card}(\cdot)$, the resulting optimization problem is difficult to solve directly. To address this issue, an effective approach is to approximate the cardinality function using its convex relaxation, namely the group lasso norm. The group lasso norm not only promotes sparsity effectively but also possesses favorable mathematical properties, enabling the transformation of the problem into a tractable convex optimization form. Accordingly, the optimization problem can be expressed as

$$\min_{K_{k+1}} f(K_{k+1}) + \gamma h(K_{k+1}) \quad (26)$$

where

$$\begin{aligned} f(K_k) &\triangleq \text{Tr}(\vec{K}_k \Psi_k \Psi_k^T \vec{K}_k^T + K_k R_k R_k^T K_k^T + K_k \Delta_k \Delta_k^T K_k^T) \\ h(K_k) &\triangleq \sum_{i=1}^M \tau_i \|K_{i,k}\|_2 \end{aligned}$$

with $\tau_i \geq 0$ being the weight parameter. Furthermore, the alternating direction method of multipliers (ADMM) [4] is employed to efficiently solve the optimization problem (26).

With the introduction of a new variable L_k , optimization problem (26) is equivalently reformulated as the following constrained optimization problem:

$$\begin{aligned} \min_{K_{k+1}, L_{k+1}} \quad & f(K_{k+1}) + \gamma h(L_{k+1}) \\ \text{s.t.} \quad & K_{k+1} = L_{k+1}. \end{aligned} \quad (27)$$

For constrained optimization problem (26), the corresponding augmented Lagrangian function is formulated as follows:

$$\begin{aligned} \mathcal{L}(K_{k+1}, L_{k+1}, \Lambda_{k+1}) \\ = f(K_{k+1}) + \gamma h(L_{k+1}) + \text{Tr}(\Lambda_{k+1}^T (K_{k+1} - L_{k+1})) \\ + \frac{\phi}{2} \|K_{k+1} - L_{k+1}\|_F^2 \end{aligned} \quad (28)$$

where Λ_k is the Lagrange multiplier and $\phi > 0$ is the penalty parameter. Following the ADMM framework, the augmented Lagrangian function is minimized through three alternating update steps (namely, K -minimization step, L -minimization step, and dual variable update step), with the $(t+1)$ -th iteration given by

$$K_{k+1}^{(t+1)} = \arg \min_{K_{k+1}} \mathcal{L}(K_{k+1}, L_{k+1}^{(t)}, \Lambda_{k+1}^{(t)}) \quad (29)$$

$$L_{k+1}^{(t+1)} = \arg \min_{L_{k+1}} \mathcal{L}(K_{k+1}^{(t+1)}, L_{k+1}, \Lambda_{k+1}^{(t)}) \quad (30)$$

$$\Lambda_{k+1}^{(t+1)} = \Lambda_{k+1}^{(t)} + \phi(K_{k+1}^{(t+1)} - L_{k+1}^{(t+1)}). \quad (31)$$

The iterative procedure terminates when either of the following conditions holds:

$$\max \{ \|K_{k+1}^{(t+1)} - L_{k+1}^{(t+1)}\|_F, \|L_{k+1}^{(t+1)} - L_{k+1}^{(t)}\|_F \} \leq \epsilon \quad (32)$$

where $\epsilon \geq 0$ is the known scalar, or when the iteration index t exceeds the maximum number of iterations t_{final} .

Subsequently, by comprehensively considering the effects of secret sharing mechanism and noise, the optimization procedures presented in (29)–(31) are analyzed in detail, and the corresponding solution results are derived.

A. K -Minimization Step Under Secret Sharing Scheme

The following theorem provides the analytical result of the K -minimization step under the secret sharing scheme.

Theorem 1: The solution to the optimization problem (29) is given by

$$\begin{aligned} K_{k+1}^{(t+1)} &= (\Psi_{k+1} \Psi_{k+1}^T C^T - \frac{1}{2} \Lambda_{k+1}^{(t)} + \frac{\phi}{2} L_{k+1}^{(t)}) \\ &\quad \times (C \Psi_{k+1} \Psi_{k+1}^T C^T + (R_{k+1} R_{k+1}^T \\ &\quad + \Delta_{k+1} \Delta_{k+1}^T) + \frac{\phi}{2} I)^{-1}. \end{aligned} \quad (33)$$

Proof: First, it follows from (28) and (29) that

$$\begin{aligned} \mathcal{L}(K_{k+1}, L_{k+1}^{(t)}, \Lambda_{k+1}^{(t)}) \\ = \text{Tr}((I - K_{k+1} C) \Psi_{k+1} \Psi_{k+1}^T (I - K_{k+1} C)^T \\ + K_{k+1} R_{k+1} R_{k+1}^T K_{k+1}^T + K_{k+1} \Delta_{k+1} \Delta_{k+1}^T K_{k+1}^T) \\ + \gamma h(L_{k+1}^{(t)}) + \text{Tr}(\Lambda_{k+1}^{(t),T} (K_{k+1} - L_{k+1}^{(t)})) \\ + \frac{\phi}{2} \text{Tr}((K_{k+1} - L_{k+1}^{(t)})(K_{k+1} - L_{k+1}^{(t)})^T). \end{aligned} \quad (34)$$

It is evident that (34) is a convex function with respect to K_{k+1} . Therefore, the optimal solution satisfies the condition that the gradient vanishes. Taking the derivative of (34) with respect to K_{k+1} yields

$$\begin{aligned} \nabla_{K_{k+1}} (\mathcal{L}(K_{k+1}, L_{k+1}^{(t)}, \Lambda_{k+1}^{(t)})) \\ = 2(K_{k+1} C - I) \Psi_{k+1} \Psi_{k+1}^T C^T + 2K_{k+1} (R_{k+1} R_{k+1}^T \\ + \Delta_{k+1} \Delta_{k+1}^T) + \Lambda_{k+1}^{(t)} + \phi(K_{k+1} - L_{k+1}^{(t)}). \end{aligned} \quad (35)$$

Then, setting (35) to zero and rearranging the terms, we obtain

$$\begin{aligned} K_{k+1} (2C \Psi_{k+1} \Psi_{k+1}^T C^T + 2(R_{k+1} R_{k+1}^T + \Delta_{k+1} \Delta_{k+1}^T) \\ + \phi I) = 2\Psi_{k+1} \Psi_{k+1}^T C^T - \Lambda_{k+1}^{(t)} + \phi L_{k+1}^{(t)}, \end{aligned} \quad (36)$$

which further indicates

$$\begin{aligned} \arg \min_{K_{k+1}} \mathcal{L}(K_{k+1}, L_{k+1}^{(t)}, \Lambda_{k+1}^{(t)}) \\ = (\Psi_{k+1} \Psi_{k+1}^T C^T - \frac{1}{2} \Lambda_{k+1}^{(t)} + \frac{\phi}{2} L_{k+1}^{(t)}) (C \Psi_{k+1} \Psi_{k+1}^T C^T \\ + (R_{k+1} R_{k+1}^T + \Delta_{k+1} \Delta_{k+1}^T) + \frac{\phi}{2} I)^{-1}. \end{aligned} \quad (37)$$

Therefore, the proof is complete. $\blacksquare$

B. L -Minimization Step Under Secret Sharing Scheme

The theorem below derives the analytical formulation corresponding to the L -minimization step under the secret sharing scheme.

Theorem 2: The solution to the optimization problem (30) is given by

$$L_{i,k+1}^{(t+1)} = \max \left(1 - \frac{\gamma \tau_i}{\phi \|\Omega_{i,k+1}^{(t)}\|_2}, 0 \right) \Omega_{i,k+1}^{(t)} \quad (38)$$

for $i = 1, 2, \dots, M$, where $L_{i,k+1}^{(t+1)}$ and $\Omega_{i,k+1}^{(t)}$ represent the i -th block columns of matrices $L_{k+1}^{(t+1)}$ and $\Omega_{k+1}^{(t)}$, respectively, and $\Omega_{i,k+1}^{(t)} \triangleq K_{i,k+1}^{(t+1)} + \frac{1}{\phi} \Lambda_{i,k+1}^{(t)}$.

Proof: First, according to (28) and (30), one has

$$\begin{aligned} \mathcal{L}(K_{k+1}^{(t+1)}, L_{k+1}, \Lambda_{k+1}^{(t)}) \\ = f(K_{k+1}^{(t+1)}) + \gamma h(L_{k+1}) + \text{Tr}(\Lambda_{k+1}^{(t),T} (K_{k+1}^{(t+1)} - L_{k+1})) \\ + \frac{\phi}{2} \|K_{k+1}^{(t+1)} - L_{k+1}\|_F^2 \\ = \gamma \sum_{i=1}^M \tau_i \|L_{i,k+1}\|_2 + \frac{\phi}{2} (\|K_{k+1}^{(t+1)} - L_{k+1}\|_F^2 \\ + \frac{2}{\phi} \text{Tr}(\Lambda_{k+1}^{(t),T} (K_{k+1}^{(t+1)} - L_{k+1})) + \|\frac{1}{\phi} \Lambda_{k+1}^{(t)}\|_F^2 \\ - \|\frac{1}{\phi} \Lambda_{k+1}^{(t)}\|_F^2) + f(K_{k+1}^{(t+1)}) \\ = \gamma \sum_{i=1}^M \tau_i \|L_{i,k+1}\|_2 + \frac{\phi}{2} \|L_{k+1} - K_{k+1}^{(t+1)} - \frac{1}{\phi} \Lambda_{k+1}^{(t)}\|_F^2 \\ - \frac{\phi}{2} \|\frac{1}{\phi} \Lambda_{k+1}^{(t)}\|_F^2 + f(K_{k+1}^{(t+1)}). \end{aligned} \quad (39)$$

Then, by applying the column-wise expansion property of the Frobenius norm, (39) is further expressed as

$$\mathcal{L}(K_{k+1}^{(t+1)}, L_{k+1}, \Lambda_{k+1}^{(t)})$$

$$= \sum_{i=1}^M \mathcal{L}_{i,k+1} - \frac{\phi}{2} \left\| \frac{1}{\phi} \Lambda_{k+1}^{(t)} \right\|_F^2 + f(K_{k+1}^{(t+1)}) \quad (40)$$

where

$$\mathcal{L}_{i,k+1} \triangleq \gamma \tau_i \|L_{i,k+1}\|_2 + \frac{\phi}{2} \|L_{i,k+1} - K_{i,k+1}^{(t+1)} - \frac{1}{\phi} \Lambda_{i,k+1}^{(t)}\|_2^2.$$

Furthermore, considering that $K_{i,k+1}^{(t+1)}$ and $\Lambda_{i,k+1}^{(t)}$ are known parameters, the solution of the optimal variable $L_{i,k+1}$ can therefore be obtained by analyzing the performance index $\mathcal{L}_{i,k+1}$ only.

The subdifferential of the objective function $\mathcal{L}_{i,k+1}$ with respect to $L_{i,k+1}$ is characterized by

$$\begin{aligned} \partial_{L_{i,k+1}} \mathcal{L}_{i,k+1} &= \begin{cases} \frac{\gamma \tau_i L_{i,k+1}}{\|L_{i,k+1}\|_2} + \phi(L_{i,k+1} - \Omega_{i,k+1}^{(t)}), & L_{i,k+1} \neq 0 \\ \gamma \tau_i \eta_{i,k+1} + \phi(L_{i,k+1} - \Omega_{i,k+1}^{(t)}), & L_{i,k+1} = 0 \end{cases} \quad (41) \end{aligned}$$

where $\Omega_{i,k+1}^{(t)} \triangleq K_{i,k+1}^{(t+1)} + \frac{1}{\phi} \Lambda_{i,k+1}^{(t)}$ and $\eta_{i,k} \triangleq \{\eta \mid \|\eta\|_2 \leq 1\}$. According to the optimality condition, we have

$$0 \in \partial_{L_{i,k+1}} \mathcal{L}_{i,k+1}. \quad (42)$$

Next, the optimal solution is analyzed by considering the following two cases: $L_{i,k+1} = 0$ is the optimal value and $L_{i,k+1} \neq 0$ is the optimal value.

Case 1: $L_{i,k+1} = 0$ is the optimal value.

In this case, the optimality condition is

$$0 \in \gamma \tau_i \eta_{i,k+1} - \phi \Omega_{i,k+1}^{(t)}, \quad (43)$$

which further shows

$$\|\Omega_{i,k+1}^{(t)}\|_2 \leq \frac{\gamma \tau_i}{\phi}. \quad (44)$$

Case 2: $L_{i,k+1} \neq 0$ is the optimal value.

When the objective function is differentiable at the considered point, the subgradient set degenerates into the ordinary gradient and the optimality condition becomes

$$\frac{\gamma \tau_i L_{i,k+1}}{\|L_{i,k+1}\|_2} + \phi(L_{i,k+1} - \Omega_{i,k+1}^{(t)}) = 0. \quad (45)$$

From (45), it follows that $L_{i,k+1}$ and $\Omega_{i,k+1}^{(t)}$ are collinear and point in the same direction. Hence, $L_{i,k+1}$ can be expressed as

$$L_{i,k+1} = \|L_{i,k+1}\|_2 \frac{\Omega_{i,k+1}^{(t)}}{\|\Omega_{i,k+1}^{(t)}\|_2}. \quad (46)$$

Then, substituting (46) into (45) results in

$$\phi \|\Omega_{i,k+1}^{(t)}\|_2 = \phi \|L_{i,k+1}\|_2 + \gamma \tau_i, \quad (47)$$

which implies

$$\|L_{i,k+1}\|_2 = \|\Omega_{i,k+1}^{(t)}\|_2 - \frac{\gamma \tau_i}{\phi} > 0. \quad (48)$$

Substituting (48) into (46) yields the optimal value for this case as

$$L_{i,k+1} = \left(1 - \frac{\gamma \tau_i}{\phi \|\Omega_{i,k+1}^{(t)}\|_2}\right) \Omega_{i,k+1}^{(t)} \quad (49)$$

with $\|\Omega_{i,k+1}^{(t)}\|_2 > \frac{\gamma \tau_i}{\phi}$.

Combining the two cases, the optimal solution can be expressed in the following form:

$$\begin{aligned} &\arg \min_{L_{k+1}} \mathcal{L}(K_{k+1}^{(t+1)}, L_{k+1}, \Lambda_{k+1}^{(t)}) \\ &= \max \left(1 - \frac{\gamma \tau_i}{\phi \|\Omega_{i,k+1}^{(t)}\|_2}, 0\right) \Omega_{i,k+1}^{(t)}, \end{aligned} \quad (50)$$

which completes the proof. $\blacksquare$

According to Theorems 1–2, the desired filter gain matrices can be obtained once the parameters determined from (33) and (38) satisfy the ADMM iteration termination condition given in (32), as presented below:

$$K_{k+1} = K_{k+1}^{(t+1)} \Pi_{k+1}^{(t+1)} \quad (51)$$

where

$$\begin{aligned} \Pi_{k+1}^{(t+1)} &\triangleq \text{diag}\{\pi_{1,k+1}^{(t+1)} I, \pi_{2,k+1}^{(t+1)} I, \dots, \pi_{M,k+1}^{(t+1)} I\} \\ \pi_{i,k+1}^{(t+1)} &= \begin{cases} 0, & 1 - \frac{\gamma \tau_i}{\phi \|\Omega_{i,k+1}^{(t)}\|_2} < 0 \\ 1, & \text{otherwise.} \end{cases} \end{aligned}$$

Moreover, for convex optimization problems, the ADMM algorithm is guaranteed to converge to the global minimum [4]. Consequently, the filter parameters given in (51) can converge to the optimal solution K_{k+1}^* of the optimization problem (26).

IV. PERFORMANCE ANALYSIS

In this section, we analyze the boundedness of the estimation error for the proposed sparsity-aware privacy-preserving zonotopic fusion filtering algorithm.

To facilitate the subsequent analysis, the decentralized privacy-preserving zonotopic filtering algorithm is first introduced. The filter structure for the i -th sensor is designed as follows:

$$\vec{x}_{i,k+1} = A \hat{x}_{i,k} \quad (52)$$

$$\hat{x}_{i,k+1} = \vec{x}_{i,k+1} + \mathcal{K}_{i,k+1} (\|y_{i,k+1}\| - C_i \vec{x}_{i,k+1}) \quad (53)$$

where $\vec{x}_{i,k}$ is the one-step prediction, $\hat{x}_{i,k}$ is the estimated state, and $\mathcal{K}_{i,k}$ is the filter parameter. Then, based on the zonotopic filtering method, the filter parameter is obtained:

$$\begin{aligned} \mathcal{K}_{i,k+1} &= \vec{\Psi}_{i,k+1} \vec{\Psi}_{i,k+1}^T C_i^T (C_i \vec{\Psi}_{i,k+1} \vec{\Psi}_{i,k+1}^T C_i^T \\ &\quad + (R_{i,k+1} R_{i,k+1}^T + \Delta_{i,k+1} \Delta_{i,k+1}^T))^{-1} \end{aligned} \quad (54)$$

where

$$\vec{P}_{i,k} = [(I - \mathcal{K}_{i,k} C_i) \vec{\Psi}_{i,k} \quad -\mathcal{K}_{i,k} R_{i,k} \quad -\mathcal{K}_{i,k} \Delta_{i,k}] \quad (55)$$

$$\vec{\Psi}_{i,k} = [A \vec{P}_{i,k-1} \quad B Q_{i,k-1}]. \quad (56)$$

Theorem 3: Suppose that (A, C_i) is observable for each $i = 1, 2, \dots, M$. Then, the optimal solution to the optimization problem (26) guarantees that the estimation error is ultimately bounded, with the bound given by

$$e_{k+1}^T e_{k+1} \leq 4 \left(\text{Tr} \left(\frac{1}{\underline{\rho}^{l+1} \underline{g}} I \right) + \gamma \bar{\tau} \sqrt{\frac{1}{\mathbf{r}} \text{Tr} \left(\frac{1}{\underline{\rho}^{l+1} \underline{g}} I \right)} \right) \quad (57)$$

where

$$1 < l < \infty, \quad 0 < g_i < \infty, \quad 0 < \rho_{i,k} < 1,$$

$$\begin{aligned}\underline{\rho} &\triangleq \min_{k \geq 0, i} \rho_{i,k}, \quad \underline{g} \triangleq \min_i g_i, \quad \bar{\tau} \triangleq \max_i \tau_i \\ \bar{b} &\triangleq \max_{k \geq 0, i} b_{i,k}, \quad \underline{\beta} \triangleq \min_i \beta_i, \quad \mathbf{r} \triangleq \left(\frac{r\beta}{2^{b-1}} \right)^2.\end{aligned}$$

Proof: First, for optimization problem (26), a feasible solution can be constructed as follows:

$$\mathcal{K}_{k+1}^f \triangleq [0 \quad \cdots \quad 0 \quad \mathcal{K}_{i,k+1} \quad 0 \quad \cdots \quad 0] \quad (58)$$

where $\mathcal{K}_{i,k+1}$ denotes the filter parameter associated with any selected sensor node. Then, according to (26) and (54)–(56), it is easy to have

$$\begin{aligned}f(K_{k+1}^*) + \gamma h(K_{k+1}^*) &\leq f(\mathcal{K}_{k+1}^f) + \gamma h(\mathcal{K}_{k+1}^f) \\ &= \text{Tr}(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T) + \gamma \tau_i \|\mathcal{K}_{i,k+1}\|_2\end{aligned} \quad (59)$$

where K_{k+1}^* denotes the optimal solution to the optimization problem (26).

By substituting (54) into (55) and utilizing the matrix inversion lemma, we readily obtain

$$\begin{aligned}(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T)^{-1} &= (\vec{\Psi}_{i,k+1} \vec{\Psi}_{i,k+1}^T)^{-1} + C_i^T (R_{i,k+1} \\ &\quad \times R_{i,k+1}^T + \Delta_{i,k+1} \Delta_{i,k+1}^T)^{-1} C_i.\end{aligned} \quad (60)$$

It follows from (56) and (60) that there exists a scalar $0 < \rho_{i,k} < 1$ such that

$$(\vec{\Psi}_{i,k+1} \vec{\Psi}_{i,k+1}^T)^{-1} \geq \rho_{i,k} A^{-1,T} (\vec{P}_{i,k} \vec{P}_{i,k}^T)^{-1} A^{-1}. \quad (61)$$

Then, from (60)–(61), one has

$$\begin{aligned}(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T)^{-1} &\geq \rho_{i,k} A^{-1,T} (\vec{P}_{i,k} \vec{P}_{i,k}^T)^{-1} A^{-1} + C_i^T (R_{i,k+1} R_{i,k+1}^T \\ &\quad + \Delta_{i,k+1} \Delta_{i,k+1}^T)^{-1} C_i \\ &\geq \rho_{i,k} \rho_{i,k-1} A^{-2,T} (\vec{P}_{i,k-1} \vec{P}_{i,k-1}^T)^{-1} A^{-2} \\ &\quad + \rho_{i,k-1} A^{-1,T} C_i^T (R_{i,k} R_{i,k}^T + \Delta_{i,k} \Delta_{i,k}^T)^{-1} C_i A^{-1} \\ &\quad + C_i^T (R_{i,k+1} R_{i,k+1}^T + \Delta_{i,k+1} \Delta_{i,k+1}^T)^{-1} C_i \\ &\vdots \\ &\geq \underline{\rho}^{l+1} \sum_{\kappa=k+1-l}^{k+1} (A^{-1,T})^{k+1-\kappa} C_i^T \mathcal{R}_{i,\kappa}^{-1} C_i (A^{-1})^{k+1-\kappa}\end{aligned} \quad (62)$$

where $\mathcal{R}_{i,\kappa} \triangleq R_{i,\kappa} R_{i,\kappa}^T + \Delta_{i,\kappa} \Delta_{i,\kappa}^T$.

Since (A, C_i) is observable, by applying the observability Gramian criterion [15], it is concluded that there exist $1 < l < \infty$ and $0 < g_i < \infty$ such that

$$\sum_{\kappa=k+1-l}^{k+1} (A^{-1,T})^{k+1-\kappa} C_i^T \mathcal{R}_{i,\kappa}^{-1} C_i (A^{-1})^{k+1-\kappa} \geq g_i I. \quad (63)$$

From (62)–(63), it is easy to derive

$$(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T)^{-1} \geq \underline{\rho}^{l+1} \underline{g} I, \quad (64)$$

which further indicates

$$\text{Tr}(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T) \leq \text{Tr}\left(\frac{1}{\underline{\rho}^{l+1} \underline{g}} I\right). \quad (65)$$

Next, according to (55), we have

$$\text{Tr}(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T) \geq \text{Tr}(\mathcal{K}_{i,k+1} \mathcal{R}_{i,k+1} \mathcal{K}_{i,k+1}^T) \quad (66)$$

which, together with Lemma 2, leads to

$$\text{Tr}(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T) \geq \mathbf{r} \|\mathcal{K}_{i,k+1}\|_F^2. \quad (67)$$

Then, it follows from (65) and (67) that

$$\|\mathcal{K}_{i,k+1}\|_F^2 \leq \frac{1}{\mathbf{r}} \text{Tr}\left(\frac{1}{\underline{\rho}^{l+1} \underline{g}} I\right), \quad (68)$$

which results in

$$\|\mathcal{K}_{i,k+1}\|_2 \leq \sqrt{\frac{1}{\mathbf{r}} \text{Tr}\left(\frac{1}{\underline{\rho}^{l+1} \underline{g}} I\right)}. \quad (69)$$

Combining (59), (65), and (69), it is easy to derive that

$$\begin{aligned}f(K_{k+1}^*) &\leq \text{Tr}(\vec{P}_{i,k+1} \vec{P}_{i,k+1}^T) + \gamma \bar{\tau} \|\mathcal{K}_{i,k+1}\|_2 \\ &\leq \text{Tr}\left(\frac{1}{\underline{\rho}^{l+1} \underline{g}} I\right) + \gamma \bar{\tau} \sqrt{\frac{1}{\mathbf{r}} \text{Tr}\left(\frac{1}{\underline{\rho}^{l+1} \underline{g}} I\right)}.\end{aligned} \quad (70)$$

Thus, we obtain (57), and the proof is complete. $\blacksquare$

V. EXPERIMENTAL VALIDATION

In this section, to verify the practical feasibility and performance of the proposed sparsity-aware privacy-preserving zonotopic fusion filtering algorithm in realistic application scenarios, experiments are carried out on a self-built automated guided vehicle (AGV) testbed.

A. Experimental Platform and Parameter Configuration

The experimental system mainly consists of an AGV, six camera sensors, and a laptop computer, where the laptop is used to emulate the cloud-side computing terminal. The overall hardware architecture of the AGV platform and the cloud computing platform are shown in Fig. 2. The deployment of the camera sensors and the motion of the AGV in the tracking experiment are illustrated in Fig. 3.

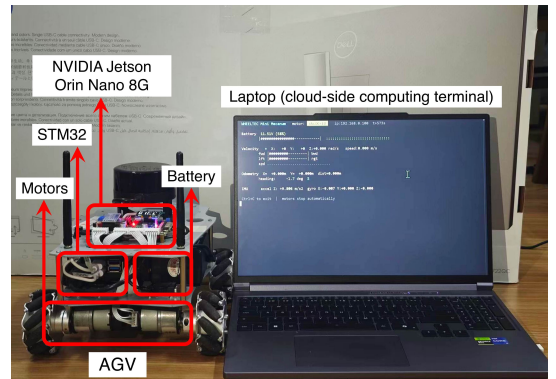


Fig. 2: The AGV platform and the laptop computer.

During the experiment, the AGV moves along the y -axis at an approximately constant speed of 0.6 m/s. The process noise during motion is modeled by a zonotope, whose shape matrix is denoted by $Q_k = \text{diag}\{0.005, 0.02 + 0.01 \sin(0.1k)\}$. Six cameras are deployed on both sides of the AGV trajectory

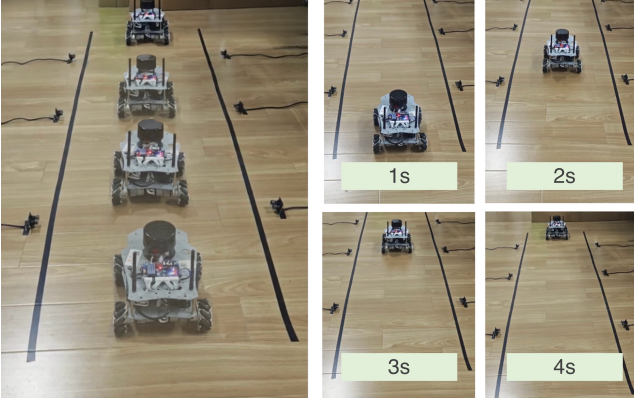


Fig. 3: The experimental process.

as roadside multi-sensor nodes. Each sensor provides two-dimensional position measurements of the AGV, with the corresponding measurement matrix given by

$$C_1 = C_2 = \dots = C_6 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Due to differences in deployment locations, calibration errors, imaging quality, and other factors, the six sensors exhibit different measurement accuracies. The shape matrices $R_{i,k}$ of the corresponding measurement-noise zonotopes are listed in Table I, where

$$\delta_{k \geq k_0} = \begin{cases} 1, & k \geq k_0 \\ 0, & \text{otherwise.} \end{cases}$$

For the dynamic-encoding-based secret sharing mechanism, the parameters are chosen as $t = 3$, $n = 5$, $r = 10$, $\alpha_i = 0.9$, $\beta_i = 1.1$, and $b_{i,k} = 12$. For the termination condition (32) of the ADMM, the parameters are set as $\epsilon = 10^{-5}$, $t_{\text{final}} = 100$, $\gamma = 1$, and $\phi = 10$.

TABLE I: Shape matrices of measurement noise

Sensor i	Shape matrix $R_{i,k}$
1	$\text{diag}\{0.02, 0.02\}$
2	$\text{diag}\{0.025 + 0.01 \sin(0.1k), 0.016\}$
3	$\text{diag}\{0.03, 0.028 + 0.01 \cos(0.1k)\}$
4	$\text{diag}\{0.045, 0.038\}$
5	$\text{diag}\{0.01, 0.01 + 0.01 \delta_{k \geq 10}\}$
6	$\text{diag}\{0.04, 0.05\}$

B. Analysis of Experimental Results

This subsection provides a comprehensive evaluation of the proposed algorithm from three perspectives: sparsity-aware state estimation, sparsity-aware sensor selection and performance comparison, and privacy-preserving performance.

1) *Sparsity-Aware State Estimation*: Figs. 4–5 present the state estimation results obtained based on camera measurement data. The proposed sparsity-aware fusion filtering algorithm is compared with the full-camera fusion filtering method. The results show that the proposed method can effectively track the actual position and velocity of the AGV using sparse camera measurements. Although only a subset of camera sensors is

activated at each sampling instant, the estimated information of p_x , p_y , v_x , and v_y remain close to those obtained by the full-camera fusion benchmark. This indicates that the proposed method can maintain satisfactory estimation performance while reducing the number of participating sensors.

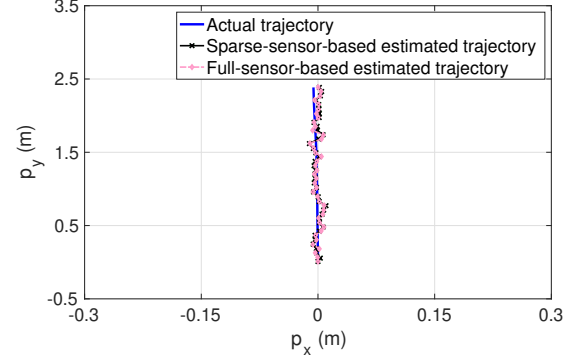


Fig. 4: Comparison between the actual AGV trajectory and the estimated trajectory.

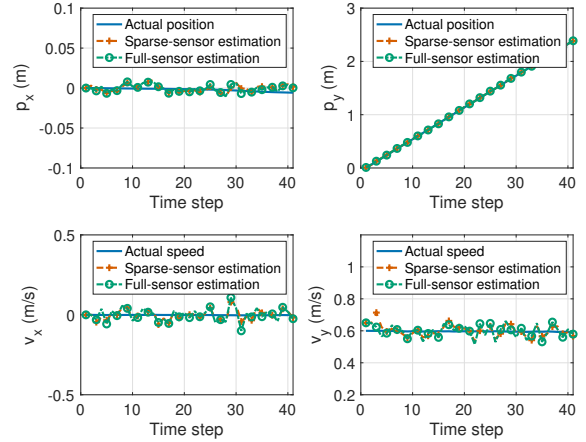


Fig. 5: Position and speed estimation of the AGV.

2) *Sparsity-Aware Sensor Selection and Performance Comparison*: Fig. 6 shows the camera sensor selection results obtained by the proposed sparsity-aware strategy. Specifically, the blue bars represent the number of activated camera sensors at each sampling instant, while the blue dashed line indicates the total number of available camera sensors, which is six in this experimental scenario. During the sparse sensor selection process, only the selected camera nodes upload the shares to the cloud platform, whereas the unselected cameras do not transmit data at the current sampling instant. Therefore, the communication overhead and the computational burden of the cloud platform can be evaluated by the number of activated camera sensors. The statistical results in Fig. 6 show that the average number of selected sensors over all sampling instants is 3.2. This indicates that the proposed sparsity-aware strategy activates, on average, only 3.2/6 of the available sensors, thereby effectively reducing both the computational burden of the cloud platform and the communication overhead.

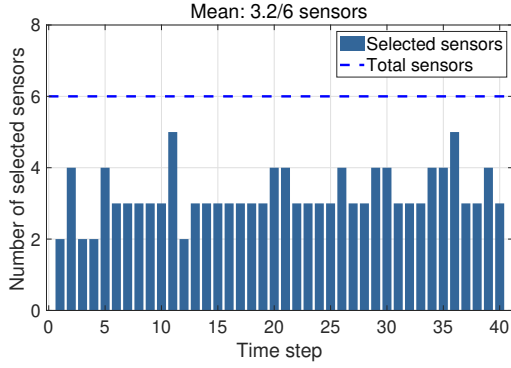


Fig. 6: Camera sensor selection results.

In addition, in the sparse sensor selection scheme, the parameter γ is used to regulate the sparsity level of the sensor selection result. Specifically, a larger γ imposes a stronger penalty on the number of selected sensors, and therefore generally leads to a sparser selection result; a smaller γ weakens this penalty and accordingly allows more sensors to be selected. When γ is set to 0, 0.5, and 5, the average numbers of selected sensors are 5, 4, and 1.6, respectively. These results indicate that the adopted sparse optimization algorithm can effectively control the number of selected sensors by tuning the parameter γ , thereby providing a basis for parameter selection under different communication-resource constraints.

To further evaluate the estimation performance of the proposed sparsity-aware filtering algorithm, $N_m = 100$ independent Monte Carlo simulations are conducted. The root mean square error (RMSE) metric is defined as follows:

$$\text{RMSE} = \sqrt{\frac{1}{N_m} \frac{1}{N_k} \sum_{m=1}^{N_m} \sum_{k=1}^{N_k} \|e_k^{[m]}\|_2^2}$$

where $e_k^{[m]}$ denotes the estimation error in the m -th experiment. To quantitatively evaluate the trade-off between estimation accuracy and communication efficiency, Table II summarizes the key performance metrics of the proposed sparsity-aware zonotopic fusion filtering algorithm and the full-sensor baseline. The proposed algorithm activates an average of 3.2 out of 6 available sensors per time step, achieving a 46.67% reduction in communication overhead relative to the full-sensor scheme, i.e., $\eta_{\text{comm}} = \frac{6-3.2}{6} \times 100\%$. In terms of estimation accuracy, the RMSE of the sparse-sensor method is 0.1267, compared to 0.1171 for the full-sensor baseline, corresponding to a marginal RMSE degradation of only 8.20%, i.e., $\eta_{\text{RMSE}} = \frac{0.1267-0.1171}{0.1171} \times 100\%$.

These results indicate that the proposed algorithm achieves an estimation accuracy comparable to the full-sensor scheme while substantially reducing the communication overhead between sensors and the cloud platform, thereby demonstrating its effectiveness and practical value in privacy-preserving cloud-based vehicle tracking systems.

TABLE II: Performance comparison of the proposed algorithm and the full-sensor baseline

Metric	Full-sensor	Sparse-sensor
Active sensors	6	4
RMSE	0.1171	0.1267
η_{comm}	—	46.67%
η_{RMSE}	—	8.20%

3) *Privacy-Preserving Performance*: To evaluate the privacy-preserving capability of the proposed framework, a simulation is conducted in which an external eavesdropper attempts to reconstruct AGV states using the observation data intercepted from the communication links. Fig. 7 shows the AGV position and velocity estimation errors obtained by the eavesdropper's filter. It is assumed that the attacker has access to information about the AGV and the camera sensors, and the attacker's filter is constructed within a zonotopic filtering framework. The estimation errors of all four state components exhibit a divergent tendency, with magnitudes reaching up to 10^4 , which stands in sharp contrast to the bounded errors achieved by the legitimate filter. The above results demonstrate that under the secret-sharing-based filtering framework, the eavesdropper is unable to obtain meaningful state estimates, highlighting the reliable privacy-preserving capability of the proposed method in cloud-based vehicle tracking systems.

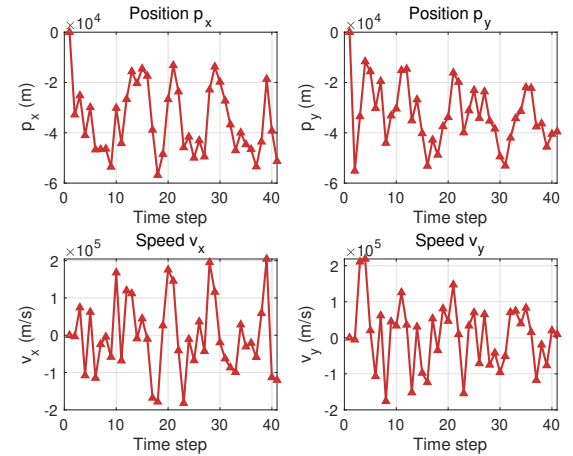


Fig. 7: State estimation errors of the external eavesdropper.

VI. CONCLUSION

In this paper, a secret-sharing-based zonotopic fusion filtering framework has been developed for cloud-based vehicle tracking systems subject to communication constraints and privacy leakage risks. First, a dynamic-encoding-based secret sharing mechanism has been introduced to ensure the security of data transmission and the privacy of estimation results. Second, a sparsity-aware sensor selection strategy has been developed to reduce unnecessary communication overhead and improve the utilization efficiency of limited bandwidth resources. The sparsity-aware optimization problem has been effectively solved by combining convex relaxation with the

ADMM, based on which analytical expressions for the filter parameters and the corresponding sensor selection strategy have been obtained. At last, a sufficient condition has been provided to guarantee the boundedness of the estimation error.

The problem of vehicle state estimation in vehicle-road-cloud systems under communication constraints and eavesdropping threats is of significant research importance. Within this research context, several complex and critical challenges remain, such as vehicle state estimation in complex traffic scenarios involving sudden acceleration or deceleration, sharp turns, and other highly dynamic maneuvers. Future work will further extend the proposed framework to more sophisticated vehicle motion models, such as constant-acceleration models, nonlinear vehicle dynamics models, and interaction-aware multi-vehicle models. In addition, appropriate nonlinear filtering methods or learning-based estimation approaches will be incorporated to improve the applicability and robustness of the proposed framework in complex traffic scenarios.

APPENDIX A PROOF OF LEMMA 2

Proof: First, by employing the mathematical induction method, we aim to prove that $\chi_{i,k}^{[\ell]} = \llbracket y_{i,k}^{[\ell]} \rrbracket$ is satisfied for any $k \geq 0$. The specific initial step and inductive step are as follows.

- 1) Initial step. From the initial condition given in (13), it is evident that

$$\chi_{i,0}^{[\ell]} = \llbracket y_{i,0}^{[\ell]} \rrbracket. \quad (71)$$

- 2) Inductive step. Suppose that $\chi_{i,k-1}^{[\ell]} = \llbracket y_{i,k-1}^{[\ell]} \rrbracket$ is true. Then, according to (12) and (13), we have

$$\begin{aligned} \chi_{i,k}^{[\ell]} - \llbracket y_{i,k}^{[\ell]} \rrbracket &= \frac{r\beta_i}{2^{b_{i,k}-1}} \left[\frac{2^{b_{i,k}-1}}{r\beta_i} (y_{i,k}^{[\ell]} - \alpha_i \chi_{i,k-1}^{[\ell]}) \right] \\ &\quad - \frac{r\beta_i}{2^{b_{i,k}-1}} (\text{Int}(y_{i,k}^{[\ell]}) - 2^{b_{i,k}-1} + 1) \\ &= 0, \end{aligned} \quad (72)$$

which implies that $\chi_{i,k}^{[\ell]} = \llbracket y_{i,k}^{[\ell]} \rrbracket$ holds.

Accordingly, by combining (71)–(72) and applying the principle of mathematical induction, it is concluded that

$$\chi_{i,k}^{[\ell]} = \llbracket y_{i,k}^{[\ell]} \rrbracket \quad (73)$$

holds for any $k \geq 0$.

Next, based on (73), it is straightforward to obtain that

$$\begin{aligned} \llbracket y_{i,k}^{[\ell]} \rrbracket - y_{i,k}^{[\ell]} &= \frac{r\beta_i}{2^{b_{i,k}-1}} \left(\left[\frac{2^{b_{i,k}-1}}{r\beta_i} (y_{i,k}^{[\ell]} - \alpha_i \chi_{i,k-1}^{[\ell]}) \right] \right. \\ &\quad \left. - \frac{2^{b_{i,k}-1}}{r\beta_i} (y_{i,k}^{[\ell]} - \alpha_i \chi_{i,k-1}^{[\ell]}) \right). \end{aligned} \quad (74)$$

Then, based on the fundamental properties of the ceiling function, it follows from (74) that

$$0 \leq \llbracket y_{i,k}^{[\ell]} \rrbracket - y_{i,k}^{[\ell]} < \frac{r\beta_i}{2^{b_{i,k}-1}}, \quad (75)$$

which further indicates (23). Thus, the proof is now complete. ■

APPENDIX B PROOF OF LEMMA 3

Proof: It follows from (17) and Lemma 1 that

$$A\langle 0, P_k \rangle \oplus \langle 0, BQ_k \rangle = \langle 0, \Psi_{k+1} \rangle, \quad (76)$$

which, combined with (17) again, demonstrates

$$\vec{e}_{k+1} \in \langle 0, \Psi_{k+1} \rangle. \quad (77)$$

Similarly, based on Lemma 1, (18), and (77), it is derived that

$$\begin{aligned} (I - K_{k+1}C)\langle 0, \Psi_{k+1} \rangle \oplus (-K_{k+1})\langle 0, R_{k+1} \rangle \\ \oplus (-K_{k+1})\langle 0, \Delta_{k+1} \rangle = \langle 0, P_{k+1} \rangle. \end{aligned} \quad (78)$$

Then, according to (18) and (78), it is obvious that

$$e_{k+1} \in \langle 0, P_{k+1} \rangle, \quad (79)$$

which completes the proof. ■

REFERENCES

- [1] A. Ahmed Amin, A. Mubarak and H. U. Manzoor, Design of intelligent vehicular and sensor communication network: A comprehensive survey, *Systems Science & Control Engineering*, vol. 13, no. 1, 2025, Art. no. 2529187.
- [2] T. Alamo, J. M. Bravo, and E. F. Camacho, Guaranteed state estimation by zonotopes, *Automatica*, vol. 41, no. 6, pp. 1035–1043, 2005.
- [3] J. Bai, Y. Zhu and G. Guo, Target tracking control of multiple unmanned surface vehicles based on distributed extended state observer, *International Journal of Systems Science*, vol. 56, no. 7, pp. 1590–1605, 2025.
- [4] S. Boyd, N. Parikh, E. Chu, B. Peleato and J. Eckstein, Distributed optimization and statistical learning with alternating direction method of multipliers, *Foundations and Trends in Machine learning*, vol. 3, no. 1, pp. 1–122, 2011.
- [5] R. Caballero-Águila, M. P. Frías-Bustamante and A. Oya-Lechuga, Least-squares linear estimation for multirate uncertain systems subject to DoS attacks, *International Journal of Network Dynamics and Intelligence*, vol. 4, no. 2, 2025, Art. no. 100014.
- [6] S. Cai, J. Liang, W. Xu, K. Yuan and J. Lu, Recursive filter design for discrete-time systems with sparsity constraint and correlated noises, In *Proceedings of 13th International Conference on Information Science and Technology*, pp. 136–141, 2023.
- [7] D. Ding, Q.-L. Han, X. Ge, X.-M. Zhang and J. Wang, Privacy-preserving filtering, control and optimization for industrial cyber-physical systems, *Science China Information Sciences*, vol. 68, no. 4, pp. 1–17, 2025.
- [8] B. Gao, J. Liu, H. Zou, J. Chen, L. He and K. Li, Vehicle-road-cloud collaborative perception framework and key technologies: A review, *IEEE Transactions on Intelligent Transportation Systems*, vol. 25, no. 2, pp. 19295–19318, 2024.
- [9] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding and F. Yang, Distributed event-triggered estimation over sensor networks: A survey, *IEEE Transactions on Cybernetics*, vol. 50, no. 3, pp. 1306–1320, 2020.
- [10] J. Hu, J. Li, C. Jia, X. Yi and H. Liu, A recursive method to encryption-decryption-based distributed set-membership filtering for time-varying saturated systems over sensor networks, *IEEE/CAA Journal of Automatica Sinica*, vol. 12, no. 5, pp. 1047–1049, 2025.
- [11] Y. Hu, C. Zhang and S. Liu, Privacy-preserving distributed recursive filtering for state-saturated systems with quantization effects, *International Journal of Network Dynamics and Intelligence*, vol. 4, no. 2, 2025, Art. no. 100012.
- [12] W. Kühn, Rigorously computed orbits of dynamical systems without the wrapping effect, *Computing*, vol. 61, no. 1, pp. 47–67, 1998.
- [13] L. Lan, G. Wei, D. Ding and J. Zhang, Zonotopic distributed fusion over binary sensor networks with bit rate allocation: A coding-decoding approach, *IEEE Transactions on Cybernetics*, vol. 54, no. 11, pp. 6855–6866, 2024.
- [14] V. T. H. Le, C. Stoica, T. Alamo, E. F. Camacho and D. Dumur, *Zonotopes: From Guaranteed State-Estimation to Control*, John Wiley & Sons, 2013.
- [15] F. L. Lewis, L. Xie and D. Popa, *Optimal and Robust Estimation: With an Introduction to Stochastic Control Theory*, CRC Press, 2017.

- [16] S. Liu, Y. Hua, Q.-L. Han and L. Xie, Distributed optimization under information constraints: A survey, *IEEE Transactions on Industrial Informatics*, vol. 22, no. 4, pp. 2653–2666, 2026.
- [17] S. Liu, L. Wang, Y. Zhang and Y.-A. Wang, Recursive filtering of networked systems with communication protocol scheduling: A survey, *International Journal of Systems Science*, vol. 55, no. 11, pp. 2499–2516, 2025.
- [18] C. Ma, P. Cheng and C. Cai, Localization and mapping method based on multimodal information fusion and deep learning for dynamic object removal, *International Journal of Network Dynamics and Intelligence*, vol. 3, no. 2, 2024, Art. no. 100008.
- [19] D. Manivannan, S. S. Moni and S. Zeadally, Secure authentication and privacy-preserving techniques in Vehicular Ad-hoc NETWORKS (VANETs), *Vehicular Communications*, vol. 25, 2020, Art. no. 100247.
- [20] E. Mousavinejad, X. Ge, Q.-L. Han, T. J. Lim and L. Vlacic, An ellipsoidal set-membership approach to distributed joint state and sensor fault estimation of autonomous ground vehicles, *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 6, pp. 1107–1118, 2021.
- [21] B. P. Nayak, L. Hota, A. Kumar, A. K. Turuk and P. H. J. Chong, Autonomous vehicles: Resource allocation, security, and data privacy, *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 1, pp. 117–131, 2022.
- [22] D. Pan, D. Ding, X. Ge, Q.-L. Han and X.-M. Zhang, Platooning control of connected automated vehicles under event-triggered and privacy-preserved communication, *IEEE Internet of Things Journal*, vol. 12, no. 24, pp. 53927–53938, 2025.
- [23] J. Pan, Q. Xu, K. Li and J. Wang, Cloud control of connected vehicle under both communication-induced sensing and control delay: A prediction method, *IEEE Transactions on Vehicular Technology*, vol. 72, no. 7, pp. 8471–8485, 2023.
- [24] H. Rowaihy, S. Eswaran, M. Johnson, D. Verma, A. Bar-Noy, T. Brown and T. La Porta, A survey of sensor selection schemes in wireless sensor networks, In *Proceedings of Unattended Ground, Sea, and Air Sensor Technologies and Applications IX*, vol. 6562, pp. 352–364, 2007.
- [25] A. Shamir, How to share a secret, *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.
- [26] H.-T. Sun, X. Chen, Z. Zhang, X. Ge and C. Peng, Data-driven event-triggered sliding mode secure control for autonomous vehicles under actuator attacks, *IEEE Transactions on Cybernetics*, vol. 55, no. 1, pp. 436–446, 2025.
- [27] L. Wan, H. Zhang, J. Sun and J. Ma, Constraint-based finite-time tracking control for intelligent multivehicle systems considering communication and operation restrictions, *IEEE Transactions on Industrial Informatics*, vol. 22, no. 1, pp. 198–206, 2026.
- [28] L. Wang, S. Yang, Y. Wan, W. Xu and M.-L. Zhang, Privacy preserving decentralized learning with positive-incentive noise, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, in press, DOI: 10.1109/TPAMI.2026.3672569.
- [29] X. Wang, M. Zhang, S. Yue, K. Li and D. Ding, Platooning control of connected automated vehicles under communication constraints: Advances and challenges, *Systems Science & Control Engineering*, vol. 14, no. 1, 2026, Art. no. 2672175.
- [30] Z. Wang, C. Xu, Z. Liu and Y. Shen, Fault detection for satellite reaction wheel based on zonotopic set-membership estimation, *IEEE Transactions on Aerospace and Electronic Systems*, vol. 61, no. 2, pp. 1577–1588, 2025.
- [31] S. Xiao, X. Ge, Q.-L. Han and Y. Zhang, Secure and collision-free multi-platoon control of automated vehicles under data falsification attacks, *Automatica*, vol. 145, 2022, Art. no. 110531.
- [32] S. Xiao, X. Ge, Q. Wu and L. Ding, Co-design of bandwidth-aware communication scheduler and cruise controller for multiple high-speed trains, *IEEE Transactions on Vehicular Technology*, vol. 73, no. 4, pp. 4993–5004, 2024.
- [33] C. Yang, J. Liang and Z. Zhao, Zonotopic distributed fusion filtering for 2-D nonlinear systems over sensor networks: A channel-based bit rate constraint, *IEEE Transactions on Signal Processing*, vol. 73, pp. 4654–4668, 2025.
- [34] H. Yang, S. Yin, H. Han and H. Sun, Sparse actuator and sensor attacks reconstruction for linear cyber-physical systems with sliding mode observer, *IEEE Transactions on Industrial Informatics*, vol. 18, no. 6, pp. 3873–3884, 2022.
- [35] K. Yang, X. Tang, J. Li, H. Wang, G. Zhong, J. Chen and D. Cao, Uncertainties in onboard algorithms for autonomous vehicles: Challenges, mitigation, and perspectives, *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 9, pp. 8963–8987, 2023.
- [36] Y. Yang, K. Yang, W. Yue, Z. Li and C. Deng, Differentially private dynamic average consensus of multiagent systems via cloud access with self-triggered mechanism, *IEEE Transactions on Control of Network Systems*, vol. 12, no. 3, pp. 2115–2127, 2025.
- [37] J. Yin, F. Yan, Y. Liu, G. He and Y. Zhuang, An overview of simultaneous localisation and mapping: towards multi-sensor fusion, *International Journal of Systems Science*, vol. 55, no. 3, pp. 550–568, 2024.
- [38] W. Yue, H. Chu, Y. Qiu and C. Dou, Efficient and secure distributed informational interaction algorithm for current sharing and voltage regulation in DC microgrids: An event-triggered differential privacy approach, *IEEE Transactions on Industrial Informatics*, in press, DOI: 10.1109/TII.2026.3675733.
- [39] S. Zhang, S. Ifqir and V. Puig, Robust LPV fault tolerant tracking control using set-based approaches for autonomous vehicles, In *Proceedings of 6th International Conference on Control and Fault-Tolerant Systems*, pp. 240–245, 2025.
- [40] K. Zhu, Z. Wang, Z. Li and C.-Z. Xu, Distributed state estimation for autonomous vehicles in unknown environments: Enhancing situational awareness, *Automatica*, vol. 189, 2026, Art. no. 113039.