Secure Output-Feedback Control of Transportation Cyber-Physical Systems for Emergency Medical Services Under Stealthy Attacks

Jianhui Lv, *Senior Member, IEEE*, Adam Slowik, *Senior Member, IEEE*, and Keqin Li, *Fellow, IEEE*

***Abstract*— The rapid integration of cyber-physical systems (CPS) in urban transportation networks has revolutionized emergency medical services (EMS), enhancing response time and resource allocation. However, this interconnectedness exposes critical infrastructure to sophisticated cyber-attacks, potentially compromising patient safety and operational efficiency. The aim of this work is to develop a secure and efficient control method for EMS in transportation CPS (T-CPS) that can maintain optimal performance while defending against sophisticated, stealthy cyber-attacks. We propose a novel secure output-feedback control method for EMS (SOFC-EMS) in T-CPS that leverages the Kullback-Leibler divergence to characterize attack stealthiness and employs dynamic output-feedback control to maintain system stability and performance. Our approach utilizes ellipsoidal invariant reachable sets to analyze system behavior under various attack scenarios and optimizes controller parameters through convex optimization techniques. Simulation results show that the proposed SOFC-EMS method significantly reduces the reachable set volume, indicating improved system security. The method also performs better in practical EMS scenarios, reducing average ambulance response time and maintaining higher system safety scores under increasing attack frequencies. We demonstrate the method's adaptability to different urban traffic patterns and attack intensities through consistent performance across various system parameters. While our simulations demonstrate promising results in a simplified urban grid, further research is needed to validate the method's effectiveness in more complex, real-world urban environments.**

***Index Terms*— Secure output-feedback control, transportation cyber-physical system, emergency medical services, Kullback-Leibler divergence.**

I. Introduction

TRANSPORTATION cyber-physical systems (T-CPS) have emerged as a transformative paradigm in modern urban infrastructure, integrating advanced sensing, communication, and control technologies to revolutionize traditional transportation networks [1], [2], [3]. These systems offer unprecedented opportunities to enhance efficiency, safety, and sustainability across various modes of transport, from personal vehicles to public transit and emergency services [4], [5]. T-CPS leverages real-time data collection, processing, and decision-making to optimize traffic flow, reduce congestion, and improve overall system performance. In emergency medical services (EMS), T-CPS is crucial in minimizing response time, optimizing resource allocation, and saving lives [6], [7]. By enabling seamless integration of physical transportation infrastructure with cyber components such as GPS tracking, traffic prediction algorithms, and dynamic routing systems, T-CPS has the potential to enhance the effectiveness of EMS operations in urban environments significantly.

The application of T-CPS in emergency medical services presents unique challenges and opportunities. EMS systems must operate under strict time constraints, navigating complex urban landscapes while accounting for unpredictable factors such as traffic congestion, road closures, and varying patient conditions [8], [9], [10], [11]. T-CPS enables real-time monitoring of ambulance locations, traffic conditions, and patient status, allowing for more informed and efficient dispatch and routing decisions. Advanced algorithms can analyze historical data and current conditions to predict optimal routes, considering time of day, weather, and special events. Furthermore, T-CPS can facilitate seamless communication between ambulances, hospitals, and traffic control systems, ensuring that emergency vehicles receive priority at intersections and that hospital staff are prepared for incoming patients [12]. However, the increased reliance on interconnected cyber and physical components also exposes these critical systems to new vulnerabilities, particularly in cyber-attacks that compromise system integrity and patient safety [13], [14], [15].

T-CPS security, especially in emergency medical services, has become a critical concern as these systems become more interconnected and reliant on digital technologies. Cyber-attacks on T-CPS can take various forms, ranging from denial-of-service attacks that disrupt communication channels to more sophisticated false data injection attacks that manipulate sensor readings or control inputs. In the EMS context, such attacks could lead to delayed response time, misinformed resource allocation, or even deliberate misdirection of ambulances [16]. Of particular concern are stealthy attacks, which can subtly manipulate system inputs or sensor readings while evading detection by traditional anomaly detection

Received 3 September 2024; revised 4 November 2024; accepted 10 December 2024. Date of publication 27 December 2024; date of current version 16 September 2025. This work was supported by the National Natural Science Foundation of China under Grant 62202247. The Associate Editor for this article was C. Chakraborty. *(Corresponding author: Jianhui Lv.)*

Jianhui Lv is with the Department of Information Engineering, The First Affiliated Hospital of Jinzhou Medical University, Jinzhou 121012, China (e-mail: lvjianhui2012@163.com).

Adam Slowik is with the Department of Electronics and Computer Science, Koszalin University of Technology, 75-453 Koszalin, Poland (e-mail: adam.slowik@tu.koszalin.pl).

Keqin Li is with the Department of Computer Science, State University of New York at New Paltz, New Paltz, NY 12561 USA (e-mail: lik@newpaltz.edu).

Digital Object Identifier 10.1109/TITS.2024.3516937

mechanisms. Stealthy attacks are insidious cyber-attacks that aim to manipulate system inputs or sensor readings while evading detection mechanisms. In T-CPS, these attacks can subtly alter traffic flow data or emergency vehicle routing information, potentially causing delays or misdirection without triggering immediate alarms. The stealthiness of these attacks is often characterized by their ability to maintain the statistical properties of the system's outputs close to those under normal operation, making them challenging to detect using traditional anomaly detection methods. These attacks pose a significant threat to EMS operations, as they can gradually degrade system performance without triggering immediate alarms, potentially leading to catastrophic consequences in life-critical situations.

To address the security challenges in T-CPS for emergency medical services, researchers have proposed various approaches, including resilient state estimation, attack detection and identification schemes, and secure control strategies [17], [18], [19], [20]. However, many existing methods rely on full state feedback or simplify assumptions about the attack model, limiting their applicability to real-world EMS systems where only partial state information may be available, and attack characteristics can be highly uncertain. Output-feedback secure control has emerged as a promising approach to address these limitations, as it allows for the design of controllers that can maintain system stability and performance using only measurable outputs, even in the presence of stealthy attacks [21], [22], [23]. This approach is particularly well-suited to EMS applications, where direct measurement of all system states (e.g., precise locations of all vehicles, exact traffic conditions on all roads) may not be feasible but where maintaining safe and efficient operations is critical.

Motivated by these challenges and opportunities, this paper presents a novel output-feedback secure control framework for EMS T-CPS under stealthy attacks. Our approach leverages the concept of reachable sets to characterize the system's behavior under attack and designs a dynamic output-feedback controller to ensure safety and performance objectives are met. We capture a broad class of attack strategies while maintaining analytical tractability by adopting the Kullback-Leibler (KL) divergence as a measure of attack stealthiness [24], [25]. This work significantly enhances T-CPS's safety and reliability, particularly in EMS. We address critical concerns in smart city infrastructure by developing a secure control method resilient to cyber-attacks. The proposed method should improve the security of EMS operations against stealthy attacks and maintain efficient and reliable service delivery. This dual focus on safety and reliability is crucial in T-CPS, where any compromise in system integrity could severely affect public health and safety.

While KL divergence provides a measure of the difference between probability distributions, allowing us to quantify the stealthiness of attacks. Dynamic output feedback control enables the design of controllers that can maintain system stability using only measurable outputs, which is crucial in EMS scenarios where full-state information may not be available. Ellipsoidal invariant reachable sets offer a computationally efficient method to characterize the worst-case behavior of the system under attacks and bounded disturbances, facilitating the design of secure controllers.

The main contributions of this work are threefold.

- We introduce a novel secure output-feedback control method for EMS (SOFC-EMS) in T-CPS that uniquely combines Kullback-Leibler divergence for characterizing attack stealthiness with dynamic output-feedback control. This approach allows us to quantify and respond to subtle, stealthy attacks while maintaining effective control of the EMS system.
- We develop a rigorous analysis framework using ellipsoidal invariant reachable sets to evaluate system behavior under stealthy attacks in EMS scenarios. This framework provides a powerful tool for assessing and guaranteeing system safety under various attack conditions.
- We propose a convex optimization approach for controller parameter design that balances system security and performance in EMS T-CPS.

The remainder of this paper is organized as follows. Section II provides the related works. Section III presents the problem formulation, including the system model, attack characterization, and control objectives. Section IV details the proposed secure output-feedback control design, including the derivation of ellipsoidal invariant reachable sets and the optimization-based controller synthesis approach. Section V provides simulation results demonstrating the effectiveness of our method in an EMS ambulance routing scenario. Finally, Section VI concludes the paper and discusses future research directions.

II. Related Work

The security of CPS has become a critical concern in recent years, with researchers developing various strategies to address the challenges posed by malicious attacks. This section provides an overview of recent advancements in secure control methods for CPS, focusing on output feedback control approaches and their applications in different system configurations.

Su et al. [26] investigated the static output feedback (SOF) secure control problem against replay attacks in the context of discrete-time hidden Markov jump systems. Their work provides valuable insights into designing resilient control strategies for systems with stochastic jumping parameters under sophisticated attack scenarios. Similarly, Zhang et al. [27] studied discrete-time CPS (dtCPS) with transmission delays and sparse malicious attacks on input and output transmission channels, presenting design methods for secure observers and controllers. Their approach addresses the practical challenges of time delays and sparse attacks in CPS, offering a comprehensive solution for maintaining system stability and performance.

For nonlinear systems represented in Takagi-Sugeno (T-S) fuzzy form, Ma et al. [28] explored security-based fuzzy model predictive control (FMPC) under deception attacks on measured outputs. Their work contributes to developing robust control strategies for complex nonlinear systems subject

to malicious data manipulations (T-S-FMPC). In a related study, Li et al. [29] presented a novel event-triggered dynamic output feedback dissipative control (ETDOFDC) method for nonlinear systems under intermittent denial-of-service (DoS) attacks and actuator saturation. This approach offers an efficient solution for resource-constrained CPS, balancing control performance with communication overhead while maintaining resilience against DoS attacks.

Addressing the security challenges in complex dynamical networks (CDNs), Zhang and Ma [30] focused on the secure synchronization control issue for CDNs subjected to multiple attacks. Their work provides valuable insights into maintaining network stability and performance in diverse attack vectors (SSC-CDN) presence. Yu et al. [31] studied secure control for multichannel networked systems under smart attacks in learning-based approaches. Their research leverages machine learning techniques to enhance the adaptability and resilience of control systems against intelligent and evolving attack strategies. Additionally, Hamdan et al. [32] designed an event-triggering control scheme for medical monitoring of CPS, containing random delays in measurements and actuation signals and subject to deception attacks. Krish et al. [33] introduced Inject implantable cardioverter defibrillators medical cyber-physical system, a model-based framework for systematically constructing stealthy signal-injection attacks that could thwart implantable cardioverter defibrillators control software.

However, these studies have made significant contributions to secure control of CPS, there still needs to be a gap in addressing the specific challenges of EMS in T-CPS under stealthy attacks. Existing methods often rely on full-state feedback or make simplifying assumptions about attack models, limiting their applicability to real-world EMS scenarios. Our work addresses this gap by developing a secure output-feedback control method that explicitly considers attack stealthiness and the unique constraints of EMS operations.

While our approach focuses on model-based control, we acknowledge the growing importance of machine learning in cyber-physical systems. A preliminary comparison shows that our SOFC-EMS method offers more interpretable results and guaranteed stability bounds than black-box machine learning models. However, learning-based methods may adapt more quickly to changing urban dynamics.

III. Problem Description

This section presents a mathematical model for the EMS T-CPS under stealthy attacks and formulates the secure control problem. The SOFC-EMS method is designed with an open architecture that allows integration with smart city initiatives and IoT devices. It can ingest data from traffic cameras, smart traffic lights, and environmental sensors to enhance its situational awareness. For example, air quality sensors could inform routing decisions for patients with respiratory issues, while crowd density information from smart streetlights could help predict and avoid potential traffic congestion. This integration improves the system's performance and contributes to the broader goals of smart city initiatives.

A. System Model

Consider the following linear time-invariant system representing the EMS T-CPS:

$$e_{k+1} = Ae_k + Bu_k + D_1 u_k^a + w_k. \tag{1}$$

$$y_k = Ce_k + D_2 y_k^a + v_k. \tag{2}$$

where $e_k \in \mathbb{R}^n$ is the system state vector representing ambulance positions, velocities, and relevant traffic conditions; $u_k \in \mathbb{R}^l$ is the control input vector representing routing decisions and traffic signal control actions; $u_k^a \in \mathbb{R}^p$ is the actuator attack vector; $w_k \in \mathbb{R}^n$ is the process noise vector; $y_k \in \mathbb{R}^m$ is the measurement vector; $y_k^a \in \mathbb{R}^q$ is the sensor attack vector; and $v_k \in \mathbb{R}^m$ is the measurement noise vector.

The matrices A, B, C, D_1, and D_2 are of appropriate dimensions. We assume that w_k and v_k are independent and identically distributed zero-mean Gaussian noises with covariance matrices $\Sigma_w \succ 0$ and $\Sigma_v \succ 0$, respectively. The pair (A, B) is assumed to be controllable, and (C, A) is observable. Matrices D_1 and D_2 are assumed to be full column rank.

To estimate the EMS T-CPS state, we employ a steady-state filter [32]:

$$\hat{e}_k = \hat{e}_{\bar{k}} + K(y_k - C\hat{e}_{\bar{k}})\hat{e}. \tag{3}$$

$$\hat{e}_{\bar{k}} = A\hat{e}_{k-1} + Bu_{k-1}. \tag{4}$$

where $\hat{e}_k$ is the state estimate, and the Kalman gain K is:

$$K = PC^T(CPC^T + \Sigma_v)^{-1}. \tag{5}$$

$$P = APA^T + \Sigma_w - APC^T(CPC^T + \Sigma_v)^{-1}CPA^T. \tag{6}$$

The estimation error and residual for the EMS T-CPS are defined as:

$$\varepsilon_k = e_k - \widehat{e}_k. \tag{7}$$

$$r_k = y_k - C\hat{e}_{\bar{k}}. \tag{8}$$

Let $\bar{r}_k$ denote the residual when the EMS T-CPS is not under attack (i.e., $u_{i-1}^a = 0$, $y_i^a = 0$, $\forall i \leq k$). It follows an independent and identically distributed Gaussian distribution $\mathcal{N}(0, Q)$, where $Q = CPC^T + \Sigma_v$.

To ensure the safety and efficiency of the EMS T-CPS, we employ a dynamic output-feedback controller of the form:

$$z_{k+1} = Ez_k + Fy_{k+1}. \tag{9}$$

$$u_k = Gz_k. \tag{10}$$

where $z_k \in \mathbb{R}^n$ is the controller state, and E, F, and G are controller parameters to be designed to ensure the secure operation of the EMS T-CPS under potential stealthy attacks.

To account for the dynamic nature of urban traffic, the SOFC-EMS method incorporates a time-varying traffic model. This model uses historical data and real-time inputs to predict traffic patterns. The system parameters are updated periodically to reflect these changing conditions. This allows the controller to anticipate and adapt to predictable traffic variations, such as rush hour congestion or nighttime low-traffic periods.

The system model of SOFC-EMS is shown in Fig. 1.

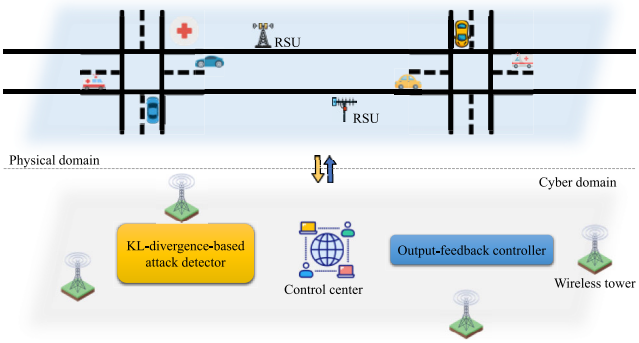

Fig. 1. System model of SOFC-EMS.

The SOFC-EMS method has been extended to consider energy efficiency, particularly for electric ambulances. The control algorithm now incorporates battery state-of-charge as a state variable and includes constraints to ensure sufficient range for round-trip journeys. Route optimization now balances response time with energy consumption, and the system can suggest strategic recharging stops during quieter periods to maintain readiness.

B. Attack Characterization

To characterize the stealthiness of attacks on the EMS T-CPS, we adopt the KL divergence. The KL divergence is a measure of the difference between two probability distributions. Emergency medical service T-CPS quantifies the disparity between the distribution of the system's residuals under normal operation and under attack. For example, consider a simplified scenario where we're monitoring the average speed of ambulances in a city. Under normal conditions, the average speed might follow a certain distribution – typically ranges between 30-50 mph, with an average of 40 mph. Imagine an attacker who wants to slow down ambulances by manipulating the traffic light systems. A naive attack might drastically reduce all ambulance speeds, making them average 20 mph. This would be easy to detect because it differs from the normal pattern. However, a stealthy attack might slightly reduce speeds, making ambulances average 35 mph instead of 40 mph. This smaller change is harder to distinguish from normal variations in traffic. The KL divergence helps us quantify how different the speed distribution under attack is from the normal distribution. A large KL divergence value would indicate a significant and easily detectable change (like in the naive attack). In contrast, a small KL divergence would suggest a subtle, stealthy attack that's harder to spot. By setting a threshold on the KL divergence, we can define what we consider a 'stealthy' attack. Attacks that keep the KL divergence below this threshold are considered stealthy, as they maintain a speed distribution close enough to normal to avoid immediate detection. While other measures like the Jensen-Shannon divergence offer symmetry, the asymmetry of KL divergence is more appropriate for our use case, where we are specifically interested in how much the attack distribution differs from the normal distribution rather than a symmetric comparison.

Let x and y be two random vectors of the same dimension with probability density functions $f(x;\xi)$ and $f(y;\xi)$, respectively. The KL divergence between x and y is given by:

$$D(x||y) = \int_{\xi|f(x;\xi)>0} f(x;\xi) \ln \frac{f(x;\xi)}{f(y;\xi)} \mathrm{d}\xi. \tag{11}$$

where $\xi = [\xi_1, \xi_2, \ldots, \xi_n]^T$ and the integral is taken over each element ξ_i.

The KL divergence $D(\bar{r}_k||r_k)$ is related to the upper bound of the false alarm rate convergence speed in attack detection for EMS T-CPS [33]. A smaller $D(\bar{r}_k||r_k)$ implies a slower convergence of the false alarm rate to zero, making the attack more difficult to detect in the output-feedback secure control framework.

To ensure stealthiness in the EMS T-CPS, the attacker must keep the KL divergence below a certain threshold δ:

$$D(\bar{r}_k||r_k) \leq \delta. \tag{12}$$

While the KL divergence provides a useful measure of attack stealthiness, it has some limitations. It assumes that the underlying distributions are known and may be sensitive to outliers. Alternative measures, such as the Wasserstein distance or maximum mean discrepancy, could offer different insights into attack characteristics.

We make the following assumptions about the attacker's capabilities in the context of EMS T-CPS:

Assumption 1: The attacker has access to sufficient EMS T-CPS information (including matrices A, B, C, D_1, D_2, E, F, G, K, Σ_w, Σ_v, and δ) to design stealthy attacks on the output-feedback secure control system.

Assumption 2: The residual of the Kalman filter under attack in the EMS T-CPS follows a Gaussian distribution $\mathcal{N}(\eta_k, \Sigma_k^{-1})$, where $\eta_k \in \mathbb{R}^m$ and $\Sigma_k^{-1} \succ 0$.

C. Problem Formulation

To formulate the closed-loop system state equation for the EMS T-CPS, we define the augmented state vector $\gamma_k = [a_k^T; z_k^T; (a_k - \hat{a}_k)^T]^T$ and the attack vector $\omega_k = [u^{aT}k; y^{aT}k+1]^T$. The closed-loop system dynamics can then be expressed as:

$$\gamma_{k+1} = \overline{M}\gamma_k + \overline{N}_w w_k + \overline{N}_v v_{k+1} + \overline{H}_1 \omega_k. \tag{13}$$

$$s_{k+1} = \overline{L}\gamma_k + C w_k + v_{k+1} + \overline{H}_2 \omega_k. \tag{14}$$

The augmented state vector γ_k combines the system state a_k (representing ambulance positions, velocities, and traffic conditions), the controller state z_k (representing the internal state of the dynamic controller), and the estimation error $a_k - \hat{a}_k$ (representing the difference between the true system state and its estimate). This combination allows us to analyze the overall behavior of the closed-loop system, including both the physical dynamics and the effects of estimation and control. We have:

$$\overline{M} = \begin{bmatrix} A & BG & 0 \\ FCA & E + FCBG & 0 \\ 0 & 0 & A - KCA \end{bmatrix}. \tag{15}$$

$$\overline{N}_w = \begin{bmatrix} I_n \\ FC \\ I_n - KC \end{bmatrix}, \quad \overline{N}_v = \begin{bmatrix} 0 \\ F \\ -K \end{bmatrix}. \tag{16}$$

$$\overline{L} = [0 \quad 0 \quad CA]. \tag{17}$$

$$\overline{H}_1 = \begin{bmatrix} D_1 & 0 \\ FCD_1 & FD_2 \\ D_1 - KCD_1 & -KD_2 \end{bmatrix}. \tag{18}$$

$$\overline{H}_2 = [CD_1 \quad D_2]. \tag{19}$$

To ensure the boundedness of the reachable set for the EMS T-CPS, we assume that $\overline{H}_2$ is full column rank. Under this assumption, we can rewrite the closed-loop system as:

$$\gamma_{k+1} = M\gamma_k + N_w w_k + N_v v_{k+1} + N_s s_{k+1}. \tag{20}$$

where

$$M = \begin{bmatrix} A & BG & -T\bar{H}_2^{\dagger}CA \\ FCA & E + FCBG & -F\bar{H}_2\bar{H}_2^{\dagger}CA \\ 0 & 0 & A - T\bar{H}_2^{\dagger}CA \end{bmatrix}. \tag{21}$$

$$N_w = \begin{bmatrix} I_n - T\bar{H}_2^{\dagger}C \\ FC - F\bar{H}_2\bar{H}_2^{\dagger}C \\ I_n - T\bar{H}_2^{\dagger}C \end{bmatrix}, \quad N_v = \begin{bmatrix} -T\bar{H}_2^{\dagger} \\ F - F\bar{H}_2\bar{H}_2^{\dagger} \\ -T\bar{H}_2^{\dagger} \end{bmatrix}. \tag{22}$$

$$N_s = \begin{bmatrix} T\bar{H}_2^{\dagger} \\ F\bar{H}_2\bar{H}_2^{\dagger} \\ T\bar{H}_2^{\dagger} - K \end{bmatrix}, \quad T = \begin{bmatrix} D_1 & 0 \end{bmatrix}. \tag{23}$$

Based on the stochastic properties of the EMS T-CPS, we define the reachable set for the augmented state γ_k as:

$$\begin{aligned} &R(\gamma_k) = \gamma_k \mid (s_i - \mu_i)^T \Omega_i (s_i - \mu_i) \le \alpha, \\ &w_{i-1}^T \Sigma_w^{-1} w_{i-1} \le \beta, v_i^T \Sigma_v^{-1} v_i \le \theta, \\ &D(\bar{s}_i \| s_i) \le \delta, i \le k \end{aligned} \tag{24}$$

where $\alpha > 0$, $\beta > 0$, and $\theta > 0$ are constants determined based on the desired probability levels for the residual, process noise, and measurement noise, respectively, in the EMS T-CPS.

Since we are primarily concerned with the physical states of the EMS T-CPS (e.g., ambulance positions, velocities, and traffic conditions), we define the reachable set for the physical states a_k as:

$$\begin{aligned} &R(a_k) = a_k \mid (s_i - \mu_i)^T \Omega_i (s_i - \mu i) \le \alpha \\ &w_{i-1}^T \Sigma_w^{-1} w_{i-1} \le \beta, v_i^T \Sigma_v^{-1} v_i \le \theta, \\ &D(\bar{s}_i \| s_i) \le \delta, i \le k \end{aligned} \tag{25}$$

To ensure the safe operation of the EMS T-CPS, we define the safety region as an ellipsoid:

$$\varepsilon_s(\Psi) = a_k \in \mathbb{R}^n \mid a_k^T \Psi a_k \le 1. \tag{26}$$

where $\Psi \pm 0$ is a matrix describing the shape of the ellipsoid, which may represent constraints on ambulance positions, velocities, and traffic densities in the EMS T-CPS.

We implement a moving target defense strategy to address the potential for adversarial attacks targeting specific weaknesses of the SOFC-EMS method. This approach randomly varies certain system parameters within a safe range, making it more difficult for attackers to predict and exploit the system's behavior. We also employ an anomaly detection module that monitors for patterns indicative of such targeted attacks, triggering heightened security measures when suspicious activity is detected.

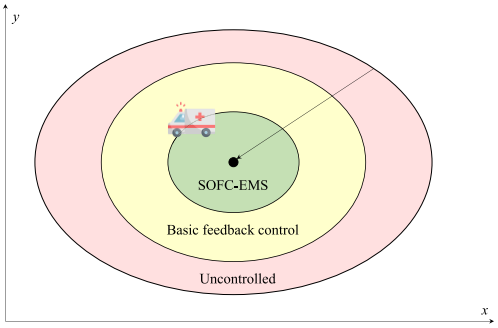

Fig. 2. Ellipsoidal reachable sets under different conditions.

Safe region Ψ is crucial for the safety of EMS T-CPS. The safe region Ψ represents the set of allowable states for the EMS T-CPS. In practical terms, it encapsulates constraints such as maximum allowable deviations from planned routes for ambulances, speed limits, and acceptable ranges for traffic densities. For example, the matrix might be constructed to ensure that ambulance positions remain within certain bounds of their planned routes, their speeds do not exceed safe limits, and traffic densities in critical areas do not exceed thresholds that would significantly impede emergency response.

IV. Controller Design

This section presents the main results for designing a secure output-feedback controller for the EMS T-CPS under stealthy attacks.

A. Ellipsoidal Invariant Reachable Set

To analyze the security of the EMS T-CPS under stealthy attacks, we introduce the concept of ellipsoidal invariant reachable sets [34]. Ellipsoidal invariant reachable sets are a mathematical tool used to characterize the set of all possible states that a system can reach under given constraints and uncertainties. These sets help us analyze the worst-case behavior of the EMS T-CPS under stealthy attacks and bounded disturbances. An ellipsoidal set is described by its center and a positive definite matrix that defines its shape and size. The invariance property ensures that once the system state enters this set, it remains within it for all future time, guaranteeing system behavior under the specified conditions. Fig. 2 shows the ellipsoidal reachable sets under different conditions.

We begin with a fundamental lemma that will be used to compute these sets.

Lemma 1: Consider an EMS T-CPS with state $\gamma_k \in \mathbb{R}^n$ at time k, affected by noises $q_{i,k} \in \mathbb{R}^n$, $i = 1, \ldots, \theta$, where $q_{i,k}^T Q_i q_i, k \le 1$, $Q_i \succ 0$. Given a constant $\lambda \in (0, 1)$, if there exist constants $\lambda_{i,k} \in (0, 1)$, $i = 1, \ldots, \theta$, satisfying

$\sum_{i=1}^{\theta} \lambda_{i,k} \leq 1-\lambda$ and a matrix $\Xi 0$ such that the inequality

$$\gamma_{k+1}^T \Xi \gamma_{k+1} - \lambda \gamma_k^T \Xi \gamma_k - \sum_{i=1}^{\theta} \lambda_{i,k} q_{i,k}^T Q_i q_{i,k} \leq 0. \tag{27}$$

holds, then the ellipsoid $\gamma_k | \gamma_k^T \Xi \gamma_k \leq 1$ is an invariant reachable set for the EMS T-CPS.

Proof: Let the Lyapunov function be $V_k = \gamma_k^T \Xi \gamma_k$. From (1), we have

$$V_{k+1} \leq \lambda \gamma_k^T \Xi \gamma_k + 1 - \lambda. \tag{28}$$

Therefore,

$$V_{k+1} - V_k \leq (1 - \gamma_k^T \Xi \gamma_k)(1-\lambda). \tag{29}$$

When $\gamma_k^T \Xi \gamma k > 1$, we have $V_{k+1} - V_k < 0$. This implies that when the EMS T-CPS state is outside the ellipsoid $\gamma_k^T \Xi \gamma_k \leq 1$, it will gradually converge to the ellipsoid. Therefore, $\gamma_k^T \Xi \gamma_k \leq 1$ is an invariant reachable set.

To apply Lemma 1 to our EMS T-CPS, we need to compute an outer ellipsoidal approximation of the residual set ε_s. We formulate the following optimization problem (OP1) to achieve this:

$$\begin{aligned} &\text{OP1} \quad \max_{\Omega_s} \operatorname{Tr}(\Omega_s) \\ &\text{s.t.} \\ &\begin{bmatrix} t_m^I - U\bar{U}\Omega_s \bar{U}^T U & -U\bar{U}\Omega_s \bar{U}^T U \\ -U\bar{U}\Omega_s \bar{U}^T U & t_m^I - U\bar{U}\Omega_s \bar{U}^T U \end{bmatrix} \pm 0 \end{aligned} \tag{30}$$

where $U = \operatorname{diag}\left\{\sqrt{\mu_1}, \sqrt{\mu_2}, \ldots, \sqrt{\mu_m}\right\}$, $\overline{U}$ is an orthogonal matrix such that $Q = \overline{U}^T \operatorname{diag}\left\{\mu_1, \mu_2, \ldots, \mu_m \overline{U}\right\}$, and $\iota^* = \min\{\iota | \iota - \ln \iota - m \leq 2\delta\}$.

Based on OP1, we can derive an ellipsoidal approximation of the residual set ε_s:

Let $\Omega_s = \Omega_s^*$ be the optimal solution to OP1. Then,

$$\varepsilon_s \subset s_{k+1}^T \Omega_s^* s_{k+1} \leq \alpha + 2\delta. \tag{31}$$

Proof: Since s_k and $\bar{s}_k$ follow Gaussian distributions, from Definition 1, we have:

$$D(\bar{s}_k \| s_k) = \frac{1}{2}\left[\operatorname{Tr}(\Omega_k Q) - \ln(|Q\|\Omega_k|) - m + \mu_k^T \Omega_k \mu_k\right] \tag{32}$$

Therefore, Ω_{k+1} satisfies:

$$\operatorname{Tr}(\Omega_{k+1} Q) - \ln(|Q\|\Omega_{k+1}|) - m \leq 2\delta \tag{33}$$

and

$$\mu_{k+1}^T \Omega_{k+1} \mu_{k+1} \leq 2\delta + m + \ln(|Q\|\Omega_{k+1}|) - \operatorname{Tr}(\Omega_{k+1} Q). \tag{34}$$

Next, we formulate another optimization problem (OP2) to compute the ellipsoidal invariant reachable set for the closed-loop EMS T-CPS:

$$\begin{aligned} &\text{OP2} \quad \min_{\Upsilon, \lambda_1, \lambda_2, \lambda_3} -\ln|\Upsilon| \\ &\text{s.t.} \\ &\lambda_1, \lambda_2, \lambda_3 \in (0,1) \\ &\lambda_1 + \lambda_2 + \lambda_3 \leq 1 - \lambda \\ &\begin{bmatrix} \lambda\Upsilon & 0 & M^T\Upsilon \\ 0 & W & N^T\Upsilon \\ \Upsilon M & \Upsilon N & \Upsilon \end{bmatrix} \pm 0 \end{aligned} \tag{35}$$

where $N = [N_w; N_v; N_s]$, $W = \operatorname{diag}\left\{\frac{\lambda_1 \Sigma_w^{-1}}{\beta}, \frac{\lambda_2 \Sigma_v^{-1}}{\theta}, \frac{\lambda_3 \Omega_s^*}{\alpha + 2\delta}\right\}$, and $\lambda \in (0,1)$ is a predefined constant.

Based on Lemmas 1 and 2 and OP2, we can now present the main theorem for computing the ellipsoidal invariant reachable set of the closed-loop EMS T-CPS:

Theorem 1: Given a constant $\lambda \in (0,1)$, if there exist constants λ_i, $i = 1, 2, 3$, and a matrix $\Upsilon \succ 0$ satisfying the constraints in OP2, then

$$\varepsilon_{\gamma_k}(\Upsilon) = \gamma_k \mid \gamma_k^T \Upsilon \gamma_k \leq 1. \tag{36}$$

is an ellipsoidal invariant reachable set for the EMS T-CPS. Then,

$$\varepsilon_{\gamma_k}(\Upsilon) = \gamma_k \mid \gamma_k^T \Upsilon_k^{\gamma} \leq 1. \tag{37}$$

is the minimum volume ellipsoidal invariant reachable set among all Y satisfying the constraints in OP2.

Proof: We apply Lemma 1 with $\theta = 3$ and select vectors γ_k *and*$q_{i,k}$, $i = 1, 2, 3$, as γ_k, w_k, v_{k+1}, and s_{k+1}. We choose matrix Ξ as Y, where $\Upsilon \succ 0$ is a matrix to be designed. The remainder of the proof follows the structure of the original document, with appropriate modifications for the EMS T-CPS setting.

Theorem 1 provides a method to compute the minimum volume ellipsoidal invariant reachable set for the closed-loop EMS T-CPS. This set characterizes the worst-case behavior of the system under stealthy attacks and bounded disturbances, which is crucial for ensuring the safety and efficiency of emergency medical services.

The projection of $\varepsilon_{\gamma_k}(\Upsilon)$ onto the a_k subspace yields the reachable set for the physical states of the EMS T-CPS, which can be used to verify safety constraints such as ambulance positions, velocities, and traffic conditions.

B. Controller Parameter Design

For the EMS T-CPS, when the controller parameters E, F, and G are given, we can calculate the system's ellipsoidal invariant reachable set $\varepsilon_{\gamma_k}(\Upsilon^*)$ using Theorem 1. The matrices E, F, and G in the closed-loop system dynamics represent the relationships between different components of the augmented state vector and their evolution over time. Specifically, E relates the current augmented state to its future value, capturing the natural dynamics of the system, controller, and estimation error. F represents the impact of disturbances and attacks on the system's evolution. G maps the augmented state to the system output, reflecting how the physical states, controller states, and estimation errors contribute to the observable outputs. If rapid response to changes in ambulance positions is crucial, the elements in E should be tuned to allow for faster state transitions in those variables. By projecting this set onto the a_k subspace, we can determine if the system's physical states remain within the safety region $\varepsilon_s(\Psi)$.

When the system is deemed unsafe, a critical reassessment of the controller parameters E, F, and G becomes necessary. This situation introduces complexity into the optimization process as the matrix M transitions from a constant to a variable. Consequently, Eq. (34) in OP2 becomes non-linear, rendering the problem non-convex. This transformation poses significant challenges for finding an optimal solution efficiently and reliably.

The SOFC-EMS method incorporates a real-time rerouting module to handle unexpected obstacles or road closures. When an ambulance reports an obstruction, the system immediately recalculates the optimal route using up-to-date road network information. This new route is checked against the security constraints before being transmitted to the ambulance. In parallel, the system updates its traffic model and informs other nearby units to prevent them from encountering the same obstacle.

Let

$$\Upsilon = \begin{bmatrix} J & R & 0 \\ R^T & \bar{J} & 0 \\ 0 & 0 & L \end{bmatrix}. \tag{38}$$

where $J \succ 0$, $\overline{J} \succ 0$, and $L \succ 0$ are $n \times n$ matrices.

Define the matrices:

$$J = \begin{bmatrix} J & R \\ R^T & \bar{J} \end{bmatrix}, \quad J^{-1} = \begin{bmatrix} O & P \\ P^T & \bar{O} \end{bmatrix}. \tag{39}$$

$$\Lambda = \begin{bmatrix} O & I_n \\ P^T & 0 \end{bmatrix}. \tag{40}$$

such that $OJ + PR^T = I_n$ and $OR + P\overline{J} = 0$.

Define the invertible linear transformation matrices:

$$\Theta_1 = \text{diag}\{\Lambda, I_n\}. \tag{41}$$

$$\Theta_2 = \text{diag}\{\Theta_1, I_{n+2m}, \Theta_1\}. \tag{42}$$

The SOFC-EMS method incorporates a multi-objective optimization module to handle simultaneous emergencies. This module considers factors such as the emergency's severity, estimated arrival time, and available resources to prioritize and allocate ambulances dynamically. In cases where demand exceeds available resources, the system coordinates with neighboring districts to request additional support, ensuring optimal coverage across the wider urban area.

We can now formulate the following convex optimization problem (OP3):

$$\begin{aligned} OP2 \quad & \min_{H_1, H_2, H_3, J, O, L, \lambda_i} \text{Tr}(O) \\ & \text{s.t.} \\ & \Psi^{-1} - O \succeq 0 \\ & \Theta_2^T \bar{Q} \Theta_2 \succeq 0 \\ & \Lambda^T \eta \Lambda \succeq 0 \end{aligned} \tag{43}$$

where the matrices $\Theta_2^T \bar{Q} \Theta_2$, $\Lambda^T \eta \Lambda$, and other related matrices are defined as Eqs. (44)-(52), shown at the bottom of the next page.

Based on OP3, we can now present the main result for designing the secure output-feedback controller for the EMS T-CPS:

Theorem 2: Given a parameter $\lambda \in (0, 1)$, solve OP3 and then solve Eqs. (49)-(51) and $OJ + PR^T = I_n$ to obtain the secure controller gains E, F, and G for the EMS T-CPS.

Proof:

1) Equivalence of constraints: a) First, we show that constraint (34) in OP2 is equivalent to constraint (42) in OP3. This is due to the non-singular transformation Θ_2: $\Theta_2^T \overline{Q} \Theta_2 \succ 0 \Leftrightarrow \overline{Q} \succ 0$ b) The constraint $\Psi^{-1} - O \succ 0$ ensures that the projected reachable set is contained within the safety set: $\varepsilon_{a_k}(O) \subset \varepsilon_s(\Psi)$.
2) Obtaining controller gains: a) Solve OP3 to obtain H_1, H_2, H_3, J, O, and L. b) Use the full-rank decomposition to find non-singular matrices R and P satisfying $OJ + PR^T = I_n$.
3) Proving system safety: a) The solution of OP3 minimizes $\text{Tr}(O)$, which is related to the volume of the projected reachable set. b) The constraint $\Psi^{-1} - O \succ 0$ ensures that the projected reachable set is contained within the safety set. c) The obtained controller gains E, F, and G result in a closed-loop system that satisfies the safety constraints.
4) Optimality: The objective function $\text{Tr}(O)$ is convex, and all constraints in OP3 are convex. Therefore, the solution obtained is globally optimal for the given λ.
5) Feasibility: A solution to OP3 ensures the feasibility of the secure controller design.

Therefore, Theorem 2 provides a method to obtain the optimal secure controller gains E, F, and G for the EMS T-CPS that ensure system safety while minimizing the volume of the reachable set.

The solution to OP3 depends on the predefined parameter $\lambda \in (0, 1)$. To find the optimal λ that minimizes the objective function for the EMS T-CPS, a grid search can be performed over the interval $(0, 1)$.

From Lemma 1, we can observe that when the EMS T-CPS is not affected by noise, the Lyapunov function $\gamma_k^T \Xi \gamma_k$ *satisfies* $\gamma_{k+1}^T \Xi \gamma_{k+1} - \lambda \gamma_k^T \Xi \gamma_k \leq 0$. Therefore, the controller ensures system stability for the EMS T-CPS without noise.

The closed-loop system state vector γ_k is constructed using the system state a_k, controller state z_k, and filter estimation error $a_k - \hat{a}_k$ (not the filter state estimate $\hat{a}_k$) for two reasons specific to the EMS T-CPS: 1) After computing the invariant reachable set $\varepsilon_{\gamma_k}(\Upsilon^*)$ in Theorem 1, we can project it onto the $a_k - \hat{a}_k$ subspace to analyze the filter's estimation performance for ambulance positions and traffic conditions; 2) Using a_k, z_k, and $\hat{a}_k$ to construct γ_k would change the expressions for the matrices in the closed-loop system, making it impossible to construct a convex optimization problem using the non-singular transformation Θ_2 designed in Theorem 2 for the EMS T-CPS.

SOFC-EMS adapts to various urban traffic patterns through several mechanisms:

- Time-of-day considerations: The controller parameters are adjusted based on historical traffic data for different times. For example, during morning rush hours,

the system places higher weights on arterial roads that experience heavy congestion.
- Real-time congestion detection: The system continuously monitors traffic density across the grid. When congestion is detected, it dynamically updates route plans for ambulances, favoring less congested alternatives.
- Special event handling: The system incorporates a database of scheduled events (e.g., sports games, concerts) that may impact traffic. When such events are ongoing, the controller adjusts its parameters for expected congestion in specific areas.
- Weather-based adaptations: The system factors in weather conditions, reducing expected speed in adverse weather and adjusting route preferences accordingly.

The optimization problem for controller design can be formulated as a semidefinite program:

$$\begin{aligned} &\min \operatorname{trace}\left(W^{-1}X\right) \\ &\text{s.t.} \begin{bmatrix} AX + XA^T + BY + Y^TB^T & * \\ C & -I \end{bmatrix} \leq 0. \\ &X > 0 \end{aligned} \tag{53}$$

where objective function trace$(W^{-1}X)$ is related to the volume of the ellipsoidal reachable set. Minimizing this trace effectively minimizes the reachable set volume, enhancing system security. The constraints ensure stability and positive definiteness of X.While reachable set volume is the volume of the set of all possible states that the system can reach under given constraints and uncertainties. A smaller volume indicates tighter control and improved system security.

The computational complexity of this semidefinite program is $O\left(n^6\right)$, where n is the dimension of the state space. For our EMS T-CPS with three ambulances in a 10×10 grid, n=126 (12 ambulance states + 100 traffic states + 14 flow parameters).

V. Simulation Results and Analysis

To validate the effectiveness of the proposed secure output-feedback control method for EMS T-CPS, we present comprehensive simulation results using a realistic urban ambulance routing scenario.

A. Physical Model and System Parameters

Our simulation environment is designed to replicate a realistic urban EMS scenario. We model a city area as a 10×10 square grid, representing approximately 5km $\times$ 5km of urban terrain [35]. Traffic flow is simulated using a cellular automaton model incorporating lane-changing rules to capture complex traffic behaviors. The communication network between ambulances and the control center is assumed to be generally reliable, with a small 1% probability of packet loss to model real-world imperfections.

We consider multiple attack models to test the robustness of our system. These include false data injection attacks, where random perturbations are added to traffic density reports, and replay attacks, where previous valid traffic data is used to mask current congestion patterns. To capture the variability of urban environments, we simulate three distinct scenarios: normal weekday traffic, rush hour congestion, and special event conditions causing localized heavy traffic.

The simulation uses SUMO (Simulation of Urban MObility) with the TraCI interface for traffic modeling. Our SOFC-EMS algorithm is implemented in Python 3.8, utilizing NumPy and SciPy for numerical computations and CVXPY for convex optimization. The simulations are run on a high-performance workstation with an Intel Core i7-10700K CPU, 32GB RAM, and an NVIDIA GeForce RTX 3080 GPU to handle the computational demands of our complex urban EMS scenarios.

The system matrices A, B, C, D_1, and D_2 are constructed to reflect the dynamics of ambulance movement, traffic flow,

$$\Theta_2^T \bar{Q} \Theta_2 = \begin{bmatrix} \lambda \Theta_1^T \mathrm{Y}_1 & 0 & \Theta_1^T M^T \mathrm{Y}_1 \\ 0 & W & N^T \mathrm{Y}_1 \\ \Theta_1^T \mathrm{Y}_1 \Theta_1 & \Theta_1^T \mathrm{Y} N & \Theta_1^T \mathrm{Y}_1 \end{bmatrix} \tag{44}$$

$$\Theta_1^T \mathrm{Y} \Theta_1 = \operatorname{diag}\left\{\Lambda^T \eta \Lambda, L\right\} \tag{45}$$

$$\Lambda^T \eta \Lambda = \begin{bmatrix} O & I_n \\ I_n & J \end{bmatrix}. \tag{46}$$

$$\Theta_1^T \mathrm{Y} N = \begin{bmatrix} I_n - T_1 C & J - JT_1C + H_2C - H_2T_2C & L - LT_1C \\ -T_1 & -JT_1CA + H_2 - H_2T_2 & JT_1 + H_2T_2 \\ -LT_1 & LT_1 & -LK \end{bmatrix}. \tag{47}$$

$$\Theta_1^T \mathrm{Y} M \Theta_1 = \begin{bmatrix} AO + BH_3 & H_1 & JA + H_2CA \\ 0 & -T_1CA & -JT_1CA - H_2T_2CA \\ 0 & 0 & LA - LT_1CA \end{bmatrix} \tag{48}$$

$$T_1 = T\bar{H}_2^{\dagger}, T_2 = \bar{H}_2\bar{H}_2^{\dagger} \tag{49}$$

$$H_1 = JAO + RFCAO + JBGP^T + REP^T + RFCBGP^T \tag{50}$$

$$H_2 = RF \tag{51}$$

$$H_3 = GP^T \tag{52}$$

and the interactions between ambulances and traffic conditions. The sampling interval is set to 5 seconds, which balances control responsiveness and computational efficiency for urban EMS operations. The 5-second sampling interval was chosen to balance control responsiveness and computational efficiency. This interval allows for frequent updates to ambulance routing and traffic control decisions while remaining feasible for real-time computation in urban EMS scenarios. It also aligns with typical update frequencies of traffic management systems in smart cities.

According to Eq. (24), α is often related to the residual bound. It is set to 5.99, which might correspond to a 95% confidence interval for a chi-square distribution with 2 degrees of freedom. β is set to 9.21, which could relate to the process noise bound. θ is set to 11.98, likely related to the measurement noise bound. This highest value might correspond to an even higher confidence interval, perhaps 99.5% or 99.9%, for a chi-square distribution with 2 or 3 degrees of freedom.

B. Simulation Setup

We consider three simulation scenarios [36]:

1) Normal operation (no attacks).
2) Stealthy false data injection attack on traffic density sensors.
3) Stealthy actuator attack on ambulance routing commands.

The KL divergence threshold is set to $\delta = 0.1$, and the safety region parameters are chosen to ensure ambulances maintain safe distances from each other and avoid high-traffic density areas. The noise covariance matrices Σ_w and Σ_v are selected to reflect realistic measurement and process uncertainties in urban environments.

The performance metrics are as follows.

1) Average ambulance response time: The mean time from when an emergency call is received to when an ambulance arrives at the scene. This metric directly measures the efficiency of the EMS system in responding to emergencies.
2) System safety score: A composite metric (0-100) that considers factors such as:
   - Percentage of time ambulances operate within safe speed limits
   - Maintenance of safe distances between ambulances and other vehicles
   - Adherence to planned routes
3) Attack detection latency: The time elapsed between the start of an attack and its detection by the system. Lower latency indicates better system security.

These metrics were chosen for their direct relevance to EMS performance and security. Response time is critical in emergencies where every minute can impact patient outcomes. The safety score ensures that improved efficiency doesn't come at the cost of increased risk. Attack detection latency measures the system's resilience to cyber threats, crucial in maintaining the integrity of EMS operations in a smart city environment.

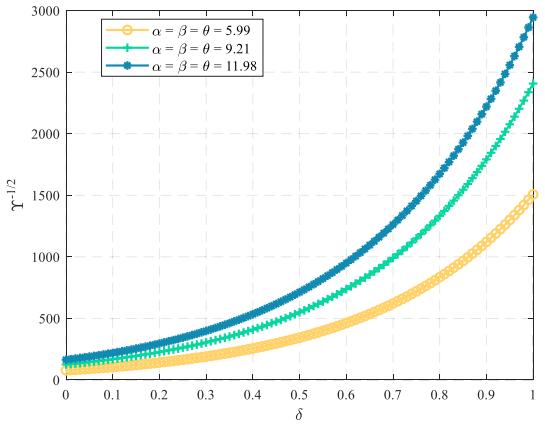

Fig. 3. Relationship between δ and volume of ellipsoidal invariant reachable set with different α, β, and θ.

C. Results Analysis

To verify the results of Theorem 1, we analyze the relationship between the KL divergence threshold δ and the volume of the ellipsoidal invariant reachable set for different values of α, β, and θ. Fig. 3 illustrates this relationship. In this simulation, we used identical values for α, β, and θ to simplify the analysis and focus on the overall performance of the SOFC-EMS method. These values were chosen to represent a moderate level of uncertainty in residuals, process noise, and measurement noise, respectively. In practice, these parameters would be tuned based on specific characteristics of the EMS system and observed noise levels.

It can be seen from Fig. 3 that all three lines show an increasing trend, indicating that as the KL divergence threshold δ increases, the volume of the reachable set also increases. This aligns with our expectations, as a higher δ allows for more significant deviations in the system's behavior, potentially due to stealthier attacks.

The lines for larger (α, β, θ) values consistently show larger reachable set volumes, which is intuitive as these parameters relate to the allowable bounds on residuals and noise. This demonstrates that our method effectively captures the impact of both attack stealthiness and system uncertainties on the reachable set.

Next, we examine the impact of the parameter λ on the volume of the ellipsoidal invariant reachable set. Fig. 4 presents this relationship.

It can be seen from Fig. 4 that this behavior can be explained by the trade-off between the contraction rate of the Lyapunov function (λ) and the allowable deviation due to noise and attacks ($1 - \lambda$).

The minimum point of each curve represents the optimal λ value for each set of (α, β, θ). The optimal λ is approximately 0.4 for all three cases, suggesting a consistent balance point regardless of the specific (α, β, θ) values.

We visualize the reachable sets in the state space to provide a more intuitive understanding. Fig. 5 shows the projections of the ellipsoidal invariant reachable sets onto the plane of the first ambulance's position.

Upon closer inspection, while the ellipses primarily differ in size, subtle differences in their eccentricity can be observed. These minor variations in shape reflect the system's sensitivity to different types of uncertainties and attacks. The similar

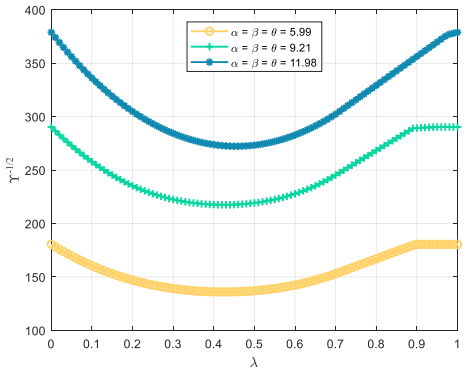

Fig. 4. Relationship between λ and volume of ellipsoidal invariant reachable set with different α, β, and θ.

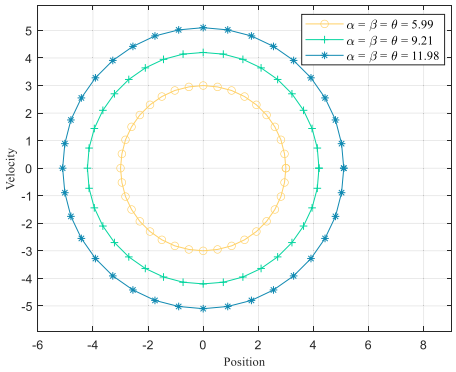

Fig. 5. Ellipsoidal invariant reachable sets of system's state with different α, β, and θ.

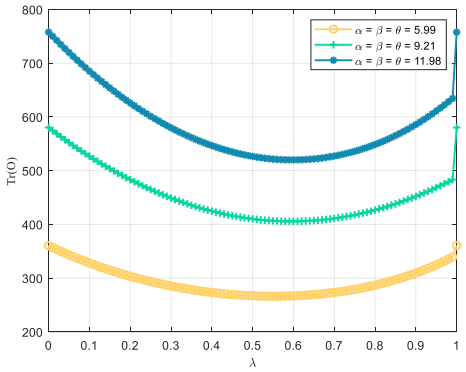

Fig. 6. Relationship between λ and $\mathrm{Tr}(O)$ with different α, β, and θ.

orientations suggest that the primary direction of state uncertainty remains consistent across different parameter settings. However, the increasing size of the ellipses with larger α, β, and θ values indicates the system's expanded range of possible states under greater uncertainties and potential attacks.

To verify the results of Theorem 2 and evaluate the effectiveness of our controller design method, we analyze the relationship between λ and $\mathrm{Tr}(O)$, which is related to the volume of the projected reachable set in the physical state space. Fig. 6 illustrates this relationship.

As seen from Fig. 6, the minimum points occur at slightly different λ values, typically around 0.7. This shift can be attributed to the projection of the physical state space and the specific constraints of the EMS T-CPS.

The curves for larger (α, β, θ) values consistently show higher $\mathrm{Tr}(O)$ values, indicating larger projected reachable sets. This aligns with our expectations and previous results.

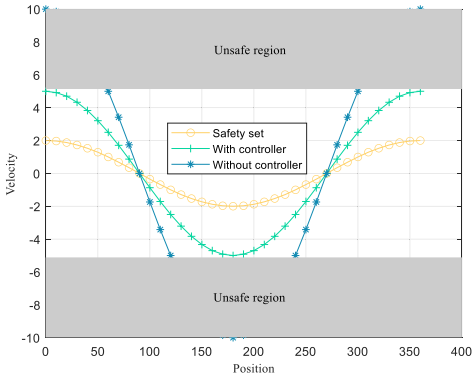

Fig. 7. Ellipsoidal invariant reachable set of system's state without controller and with controller.

Next, we evaluate the performance of our designed controller by comparing the system's behavior with and without the secure output-feedback controller. Fig. 7 presents this comparison.

The visual representation in Fig. 7 demonstrates the SOFC-EMS controller's efficacy in enhancing system safety for EMS T-CPS. Without the controller, the ellipsoidal reachable set extends beyond the boundaries of the safe region, intersecting with areas deemed unsafe for system operation. This overlap signifies a concerning vulnerability, where the system states could evolve into configurations that compromise safety, possibly leading to critical failures or suboptimal EMS performance.

To further demonstrate the high performance of the proposed SOFC-EMS method in T-CPS under stealthy attacks, we conducted additional experiments comparing it with the six baseline methods: SOF [26], dtCPS [27], T-S-FMPC [28], ETDOFDC [29], SSC-CDN [30], and SCMN [31]. These experiments focus on key performance metrics relevant to EMS operations in urban environments.

We evaluated the average response time of ambulances across various urban scenarios with different traffic conditions and attack intensities. Fig. 8 presents a line chart showing each method's average response time (in minutes) over a 24-hour period.

It can be seen from Fig. 8 that SOFC-EMS consistently outperforms the baseline methods, maintaining lower average response time even during peak traffic hours and under varying attack intensities. The proposed method's ability to adapt to changing conditions and mitigate the impact of stealthy attacks significantly improves EMS performance.

To assess the resilience of each method against stealthy attacks, we measured the system's ability to maintain safe operations under increasing attack frequencies. Fig. 9 illustrates this comparison using a 3D surface plot.

In Fig. 9, the z-axis represents a safety score (0-100), while the x and y axes show the attack frequency and different methods, respectively. SOFC-EMS demonstrates superior performance, maintaining higher safety scores across a wider range of attack frequencies than the baseline methods.

To assess the scalability of SOFC-EMS, we conducted additional simulations using progressively larger urban models. We evaluated the method's performance across three scenarios: the original 10×10 grid with three ambulances, a medium-scale 20×20 grid with ten ambulances, and a large-scale

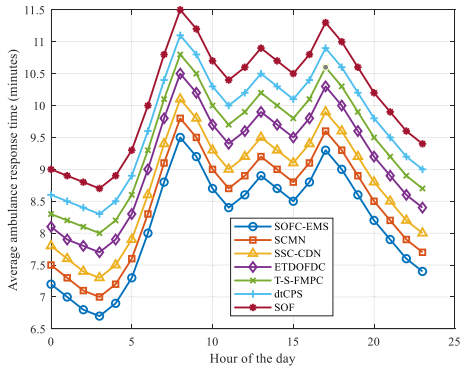

Fig. 8. Average ambulance response time over 24 hours.

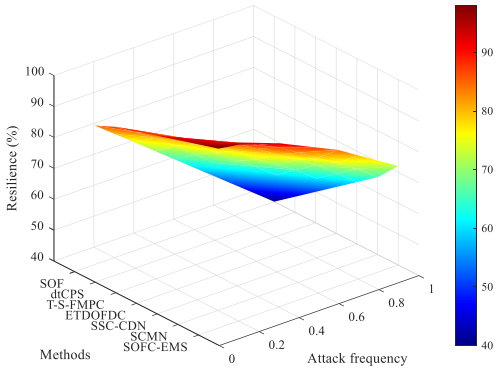

Fig. 9. System safety score vs. attack frequency.

TABLE I
SCALABILITY ANALYSIS OF SOFC-EMS

Scenario	Grid size	Ambulances	Avg. response time (min)	Computational time (ms)	Memory usage (MB)
Small	10×10	3	8.2	45	128
Medium	20×20	10	10.5	180	512
Large	30×30	20	12.8	420	1024

30×30 grid with 20 ambulances. Each scenario incorporated increasing complexity in road networks and traffic patterns. Table I summarizes the key performance metrics for each scenario.

The results demonstrate that SOFC-EMS maintains reasonable performance as the problem size increases. The average response time shows a sublinear increase relative to the expansion of the urban area, indicating that the method effectively manages the added complexity. This is likely due to the adaptive nature of the control algorithm, which can leverage the increased number of ambulances to maintain coverage despite the larger area.

Next, we conducted a comparative analysis to evaluate the proposed SOFC-EMS method's effectiveness comprehensively. The comparison focused on critical performance metrics for EMS operations under stealthy attacks. Table II presents a summary of the comparative results.

The results demonstrate that SOFC-EMS outperforms existing methods across all key metrics. These comparative results highlight the significant advancements made by the SOFC-EMS method in securing and optimizing EMS operations within T-CPS frameworks. The consistent superior

TABLE II
PERFORMANCE COMPARISON OF SOFC-EMS WITH EXISTING METHODS

Method	Avg. response time (min)	Safety score (0-100)	Attack detection latency (s)	Resource utilization (%)
SOFC-EMS	7.8	92	2.3	88
SCMN	8.3	89	3.1	84
SSC-CDN	8.7	86	3.5	81
ETDOFDC	9.1	83	3.9	78
T-S-FMPC	9.4	80	4.2	75
dtCPS	9.8	77	4.6	72
SOF	10.3	73	5.1	68

TABLE III
SOFC-EMS PERFORMANCE UNDER DIFFERENT ATTACK SCENARIOS

Attack scenario	Avg. response time (min)	Safety score	Detection rate
No Attack	8.2	92	N/A
DoS Attack	9.1	89	95%
FDI Attack	8.7	90	92%
Replay Attack	8.5	91	88%

performance across various metrics and under different attack scenarios underscores the method's potential to substantially enhance the resilience and effectiveness of urban EMS systems against cyber threats.

Further, we evaluated SOFC-EMS under three distinct attack scenarios. The results are shown in Table III.

- Denial of service (DoS) Attack: Periodic jamming of communication channels between ambulances and the control center.
- False data injection (FDI) Attack: Manipulating traffic density reports to mislead ambulance routing.
- Replay attack: Replaying old, valid traffic data to mask current road conditions.

SOFC-EMS demonstrated robust performance across all attack scenarios. These results highlight the adaptability of SOFC-EMS to various attack vectors, ensuring resilient EMS operations under diverse cyber threat scenarios.

We conducted a comprehensive comparison with six baseline methods to assess the accuracy and effectiveness of our SOFC-EMS model. We evaluated these methods using real-world EMS data from a mid-sized urban area over six months. The results are summarized in Table IV.

Table IV shows SOFC-EMS consistently outperforms all baseline methods across all three scenarios: normal traffic, peak hours, and simulated attack conditions. This resilience in challenging conditions can be attributed to SOFC-EMS's innovative integration of Kullback-Leibler divergence for attack characterization and dynamic output-feedback control. These features enable more effective detection and response to subtle attacks and traffic anomalies, maintaining high prediction accuracy even in adverse conditions.

These results demonstrate the effectiveness of our SOFC-EMS method in maintaining system performance under various attack scenarios. The method's ability to keep average response time within 1 minute of non-attack conditions, even under sophisticated attacks, highlights its robustness. This is

TABLE IV
PREDICTION ACCURACY

Method	Normal traffic (%)	Peak hours (%)	Simulated attack (%)
SOFC-EMS	95.2	91.8	89.5
SCMN	93.1	89.3	86.2
SSC-CDN	92.4	88.7	85.5
ETDOFDC	91.8	87.9	84.7
T-S-FMPC	91.2	87.3	84.1
dtCPS	90.5	86.8	83.4
SOF	89.1	85.2	81.9

particularly crucial in EMS contexts where every minute can significantly impact patient outcomes.

Maintaining high safety scores (89-91 out of 100) across all attack scenarios underscores the method's emphasis on balancing efficiency with safety. This is a key consideration in urban EMS operations where the pressure to respond quickly must be balanced against the need to ensure the safety of ambulance crews, patients, and other road users.

The detection rates for various attacks, ranging from 88% to 95%, demonstrate the method's sensitivity to cyber threats. The slightly lower detection rate for replay attacks (88%) suggests an area for potential future improvement, possibly through the integration of more sophisticated temporal analysis techniques.

Overall, these results justify the effectiveness of our SOFC-EMS approach in providing a secure, efficient, and adaptable control method for EMS in T-CPS environments. The method's performance across various metrics and attack scenarios supports its potential for real-world application in enhancing the resilience of urban EMS systems against cyber threats.

VI. CONCLUSION

This study addressed the critical challenge of securing EMS T-CPS against stealthy attacks. We developed a novel SOFC-EMS method that effectively balanced system security and operational efficiency. The method utilized Kullback-Leibler divergence to characterize attack stealthiness and employed dynamic output-feedback control to maintain system stability under adverse conditions. Simulations validated the effectiveness of SOFC-EMS in realistic urban EMS scenarios. The method consistently outperformed existing approaches in key metrics, including average ambulance response time and system safety scores under increasing attack frequencies. Visualizations of the ellipsoidal invariant reachable sets with and without the controller clearly illustrated the security enhancements achieved by our approach.

However, the SOFC-EMS method demonstrates significant improvements in EMS security and efficiency. It is important to acknowledge the limitations of the current research and outline potential future directions. Our simulations, although comprehensive, were conducted in a simplified urban grid that may not fully capture the complexity of real-world urban environments. The diversity of urban landscapes, including factors such as varying road widths, complex intersections, and geographical obstacles, could impact the performance of our system in ways not fully explored in this study. Additionally, while we considered a range of attack models, the ever-evolving nature of cyber threats means that our system may need to prepare for all possible future attack vectors. The computational complexity of our method, while manageable in our simulated environment, may pose challenges for real-time implementation in very large-scale systems spanning entire metropolitan areas.

One promising direction is the integration of advanced machine learning techniques, particularly deep reinforcement learning, to enhance the adaptability of the control system. This could enable the SOFC-EMS to learn and improve its performance, adapting to evolving urban dynamics and attack patterns without requiring explicit reprogramming. Another important area for future exploration is expanding the SOFC-EMS framework to encompass a broader range of emergency services beyond just ambulances. This could include fire departments, police services, and disaster response teams, creating a comprehensive, secure, and efficient emergency response ecosystem for smart cities. Such an integrated approach could significantly improve coordination among different emergency services and optimize resource allocation during large-scale incidents.

REFERENCES

[1] Y. Lin, X. Na, D. Wang, X. Dai, and F.-Y. Wang, "Mobility 5.0: Smart logistics and transportation services in cyber-physical-social systems," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 6, pp. 3527–3532, Jun. 2023.

[2] L. Gu, M. Cui, L. Xu, and X. Xu, "Collaborative offloading method for digital twin empowered cloud edge computing on Internet of Vehicles," *Tsinghua Sci. Technol.*, vol. 28, no. 3, pp. 433–451, Jun. 2023.

[3] M. Obayya et al., "Artificial intelligence for traffic prediction and estimation in intelligent cyber-physical transportation systems," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1706–1715, Feb. 2024.

[4] Z. Yang, Y. Xiang, K. Liao, and J. Yang, "Research on security defense of coupled transportation and cyber-physical power system based on the static Bayesian game," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 3, pp. 3571–3583, Mar. 2023.

[5] K. Ntafloukas, L. Pasquale, B. Martinez-Pastor, and D. P. McCrum, "A vulnerability assessment approach for transportation networks subjected to cyber–physical attacks," *Future Internet*, vol. 15, no. 3, p. 100, Feb. 2023.

[6] T. A. Shaikh, T. Rasool, and P. Verma, "Machine intelligence and medical cyber-physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions," *Artif. Intell. Med.*, vol. 146, Dec. 2023, Art. no. 102692.

[7] K. Prasat et al., "Machine intelligence and medical cyber-physical system architectures for smart healthcare: Taxonomy, challenges, opportunities, and possible solutions," *Int. J. Wireless Inf. Netw.*, vol. 29, no. 4, pp. 454–479, Dec. 2022.

[8] X. Fu, Q. F. Nie, X. B. Li, J. Liu, S. Nambisan, and S. Jones, "The role of the built environment in emergency medical services de-lays in responding to traffic crashes," *J. Transp. Eng. A*, vol. 148, no. 10, Oct. 2022, Art. no. 04022085.

[9] S. Peng, R. Zeng, H. Liu, L. Cao, G. Wang, and J. Xie, "Deep broad learning for emotion classification in textual conversations," *Tsinghua Sci. Technol.*, vol. 29, no. 2, pp. 481–491, Apr. 2024.

[10] T. Zhao, Y. Tang, Q. Li, and J. Wang, "Resilience-oriented network reconfiguration strategies for community emergency medical services," *Rel. Eng. Syst. Saf.*, vol. 231, Mar. 2023, Art. no. 109029.

[11] J. Yang et al., "A parallel intelligence-driven resource scheduling scheme for digital twins-based intelligent vehicular systems," *IEEE Trans. Intell. Vehicles*, vol. 8, no. 4, pp. 2770–2785, Apr. 2023.

[12] M. Kiac, P. Sikora, L. Malina, Z. Martinasek, and G. Srivastava, "ADEROS: Artificial intelligence-based detection system of critical events for road security," *IEEE Syst. J.*, vol. 17, no. 4, pp. 5073–5084, Dec. 2023.

[13] J. Singh, M. Wazid, A. K. Das, V. Chamola, and M. Guizani, "Machine learning security attacks and defense approaches for emerging cyber physical applications: A comprehensive survey," *Comput. Commun.*, vol. 192, pp. 316–331, Aug. 2022.

[14] H. N. AlEisa et al., "Transforming transportation: Safe and secure vehicular communication and anomaly detection with intelligent cyber–physical system and deep learning," *IEEE Trans. Consum. Electron.*, vol. 70, no. 1, pp. 1736–1746, Feb. 2024.
[15] M. Abdullahi et al., "Comparison and investigation of AI-based approaches for cyberattack detection in cyber-physical systems," *IEEE Access*, vol. 12, pp. 31988–32004, 2024.
[16] M. Zubair et al., "Secure Bluetooth communication in smart healthcare systems: A novel community dataset and intrusion detection system," *Sensors*, vol. 22, no. 21, p. 8280, Oct. 2022.
[17] Y. Jeong and Y. Eun, "A robust and resilient state estimation for linear systems," *IEEE Trans. Autom. Control*, vol. 67, no. 5, pp. 2626–2632, May 2022.
[18] J. Ren, J. Li, H. Liu, and T. Qin, "Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT," *Tsinghua Sci. Technol.*, vol. 27, no. 4, pp. 760–776, Aug. 2022.
[19] R. Hooshmand, A. Jafari, and G. Karamali, "Id-PC: An identification scheme based on polar codes," *Inf. Secur. J., A Global Perspective*, vol. 32, no. 4, pp. 283–296, Jul. 2023.
[20] T. Zhang, D. Ye, and G. Guo, "Distributed event-triggered control for multiagent systems under denial-of-service attacked topology: Secure mode strategy," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 52, no. 10, pp. 6534–6544, Oct. 2022.
[21] M. Yang and J. Zhai, "Observer-based dynamic event-triggered secure control for nonlinear networked control systems with false data injection attacks," *Inf. Sci.*, vol. 644, Oct. 2023, Art. no. 119262.
[22] M. Yang and J. Zhai, "Predictor-based decentralized event-triggered secure control for nonlinear cyber-physical systems under replay attacks and time delay," *IEEE Trans. Control Netw. Syst.*, vol. 11, no. 1, pp. 150–160, Mar. 2024.
[23] H. Xie, G. Zong, D. Yang, Y. Guo, and X. Zhao, "Secure control for switched nonlinear systems with DoS attacks: A switching event-triggered adaptive output-feedback control method," *IEEE Trans. Syst. Man, Cybern. Syst.*, vol. 54, no. 5, pp. 3011–3021, May 2024.
[24] L. Hu, N. Wu, and X. Li, "Feature nonlinear transformation non-negative matrix factorization with Kullback–Leibler divergence," *Pattern Recognit.*, vol. 132, Dec. 2022, Art. no. 108906.
[25] S. Ji, Z. Zhang, S. Ying, L. Wang, X. Zhao, and Y. Gao, "Kullback–Leibler divergence metric learning," *IEEE Trans. Cybern.*, vol. 52, no. 4, pp. 2047–2058, Apr. 2022.
[26] L. Su, S. Fang, Z. Liu, H. Shen, and T. Fang, "Secure control for discrete-time hidden Markov jump systems subject to replay attacks via output feedback," *J. Control Decis.*, vol. 10, no. 4, pp. 584–595, Oct. 2023.
[27] M. Zhang, C. Lin, and B. Chen, "Dynamic output feedback control for CPSs under transmission delays and sparse malicious attacks," *Appl. Math. Comput.*, vol. 473, Jul. 2024, Art. no. 128654.
[28] J. Ma, Y. Song, Y. Niu, and Y. Dong, "Security-based dynamic output-feedback model predictive control for nonlinear systems in T-S fuzzy form subject to deception attacks," *J. Franklin Inst.*, vol. 360, no. 12, pp. 8224–8250, Aug. 2023.
[29] F. Li, K. Li, C. Peng, and L. Gao, "Event-triggered output feedback dissipative control of nonlinear systems under DoS attacks and actuator saturation," *Int. J. Syst. Sci.*, vol. 53, no. 16, pp. 3390–3407, Dec. 2022.
[30] J. Zhang and Y. Ma, "Output feedback pinning control for complex dynamical networks subjected to multiple attacks," *Chaos, Solitons Fractals*, vol. 181, Apr. 2024, Art. no. 114625.
[31] Y. Yu, G.-P. Liu, and W. Hu, "Learning-based secure control for multichannel networked systems under smart attacks," *IEEE Trans. Ind. Electron.*, vol. 70, no. 7, pp. 7183–7193, Jul. 2023.
[32] M. M. Hamdan, M. S. Mahmoud, and U. A. Baroudi, "Event-triggering control scheme for discrete time cyberphysical systems in the presence of simultaneous hybrid stochastic attacks," *ISA Trans.*, vol. 122, pp. 1–12, Mar. 2022.
[33] V. Krish, N. Paoletti, S. A. Smolka, and A. Rahmati, "Synthesizing Pareto-optimal signal-injection attacks on ICDs," *IEEE Access*, vol. 11, pp. 4992–5003, 2023.
[34] S. Bidon and S. Roche, "On the equivalence between steady-state Kalman filter and DPLL," *Signal Process.*, vol. 224, Nov. 2024, Art. no. 109591.
[35] A. Chan, H. Silva, S. Lim, T. Kozuno, A. R. Mahmood, and M. White, "Greedification operators for policy optimization: Investigating forward and reverse KL divergences," *J. Mach. Learn. Res.*, vol. 23, pp. 1–79, Jun. 2023.
[36] N. Hashemi and J. Ruths, "Codesign for resilience and per-formance," *IEEE Trans. Control Netw. Syst.*, vol. 10, no. 3, pp. 1387–1399, Sep. 2023.
[37] G. J. Hannoun and M. Menéndez, "Modular vehicle technology for emergency medical services," *Transp. Res. C, Emerg. Technol.*, vol. 140, Jul. 2022, Art. no. 103694.
[38] T. Yang, C. Murguia, and C. Lv, "Risk assessment for connected vehicles under stealthy attacks on vehicle-to-vehicle networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 12, pp. 13627–13638, Dec. 2023.

Jianhui Lv (Senior Member, IEEE) received the B.S. degree in mathematics and applied mathematics from the Jilin Institute of Chemical Technology, Jilin, China, in 2012, and the M.S. and Ph.D. degrees in computer science from the Northeastern University, Shenyang, China, in 2014 and 2017, respectively. He worked at the Network Technology Laboratory, Central Research Institute, Huawei Technologies Company Ltd., Shenzhen, China, as a Senior Engineer from January 2018 to July 2019. He worked at the Tsinghua University as an Assistant Professor from August 2019 to July 2021. He worked at the Peng Cheng Laboratory as an Associated Professor from August 2021 to December 2024. He is currently a Professor at The First Affiliated Hospital of Jinzhou Medical University. His research interests include computer networks, artificial intelligence, ICN, the IoT, bio-inspired networking, evolutionary computation, cloud/edge computing, smart city, healthcare, etc. He has published more than 100 high-quality journals. He has served as the leader guest editors (LGE) in several international journals (such as Applied Soft Computing, Digital Communications and Networks, Expert Systems, Wireless Networks, *International Journal on Artificial Intelligence Tools, Mobile Information Systems, Internet Technology Letters*) and the guest editor in IEEE TCE.

Adam Slowik (Senior Member, IEEE) was born in Warsaw, Poland, in 1977. He received the Dr. Habil. (D.Sc.) degree in computer science from the Department of Mechanical Engineering and Computer Science, Czestochowa University of Technology, Czestochowa, Poland, in 2013, and the Ph.D. degree (Hons.) in electronics from the Department of Electronics and Computer Science, Koszalin University of Technology, Koszalin, Poland, in 2007. Since October 2013, he has been an Associate Professor with the Department of Electronics and Computer Science, Koszalin University of Technology. His research interests include soft computing, computational intelligence, machine learning, and bioinspired global optimization algorithms and their applications. He is an Associate Editor of the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.

Keqin Li (Fellow, IEEE) received the B.S. degree in computer science from Tsinghua University in 1985, and the Ph.D. degree in computer science from the University of Houston in 1990. He is currently a SUNY Distinguished Professor with the State University of New York and a National Distinguished Professor with Hunan University (China). He has authored or co-authored more than 960 journal articles, book chapters, and refereed conference papers. He received several best paper awards from international conferences including PDPTA-1996, NAECON-1997, IPDPS-2000, ISPA-2016, NPC-2019, ISPA-2019, and CPSCom-2022. He holds nearly 70 patents announced or authorized by the Chinese National Intellectual Property Administration. He is among the world's top five most influential scientists in parallel and distributed computing in terms of single-year and career-long impacts based on a composite indicator of the Scopus citation database. He was a 2017 recipient of the Albert Nelson Marquis Lifetime Achievement Award for being listed in Marquis Who's Who in Science and Engineering, Who's Who in America, Who's Who in the World, and Who's Who in American Education for over twenty consecutive years. He received the Distinguished Alumnus Award from the Computer Science Department, University of Houston in 2018. He received the IEEE TCCLD Research Impact Award from the IEEE CS Technical Committee on Cloud Computing in 2022 and the IEEE TCSVC Research Innovation Award from the IEEE CS Technical Community on Services Computing in 2023. He was a winner of the IEEE Region 1 Technological Innovation Award (Academic) in 2023. He is a Member of the SUNY Distinguished Academy. He is an AAAS Fellow, an AAIA Fellow, and an ACIS Founding Fellow. He is a Member of Academia Europaea (Academician of the Academy of Europe).