Adaptive Resilient Control for Cyber-Physical Systems Against Unknown Injection Attacks in Sensor Networks

Yuehui Ji (✉ jiyuehuittju@126.com)

Tianjin University of Technology <https://orcid.org/0000-0003-4815-4546>

Qiang Gao

Tianjin university of technology

Junjin Liu

Tianjin University of Technology

Research Article

Keywords: Cyber-physical Systems, False Data Injection Attacks, Resilient Control, Adaptive Control, Extended State Observers.

Posted Date: March 1st, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-204820/v1>

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
[Read Full License](#)

Adaptive Resilient Control for Cyber-physical Systems against Unknown Injection Attacks in Sensor Networks[☆]

Yuehui Ji^{*}, Qiang Gao, Junjie Liu

School of Electrical and Electronic Engineering, and Tianjin Key Laboratory for Control Theory & Applications in Complicated Systems, Tianjin University of Technology, Tianjin, 300384, China

[☆]This research was supported by Research Project of Tianjin Municipal Education Commission(Grant No. 2017KJ249)

^{*}Corresponding author: jiyuehuitju@126.com

Abstract: An adaptive resilient control is concerned for a class of cyber-physical systems(CPSs) in presence of stealthy false data injection attacks in sensor networks and unknown strict-feedback nonlinear dynamics. As the sensors are attacked by ill-disposed hackers, the exactly measured state information is unavailable for state feedback control. After theory ratiocinations, the initial issue of false data injection attacks is transformed into nonlinear uncertainty dynamics and unknown control directions at the last step. At each step in the recursive backstepping control, extended state observers(ESOs) in active disturbance rejection control(ADRC) are investigated to approximate the lumped system uncertainties. Specially, the Nussbaum functions are introduced at the last step in the adaptive control. All the closed-loop signals are proved to be semi-globally uniformly ultimately bounded by Lyapunov theory. Finally, numerical simulations verify that the proposed control can afford favorable stabilization performance and counter false data injection attack.

Keyword: Cyber-physical Systems; False Data Injection Attacks; Resilient Control; Adaptive Control; Extended State Observers.

I. Introduction

As a tight integrated system, cyber-physical systems are composed of physical elements (including controllers, sensors, actuators, plants) and cyber networks for accurate sensing, ubiquitous computation, efficient communication, effective control^[1-3]. The real application communities of CPSs cover transportation^[4,5], health monitoring^[6,7], manufacture^[8,9], smart grid^[10], aerospace system^[11], and so on. The connection to the internet in CPSs renders it is more vulnerable to malicious instructions and attacks.

According to different attack targets, the cyber-attacks can be classified into denial-of-service(DoS) attacks and deception attacks, which may deteriorate the system performance, even cause

instability. The DoS attacks attempt to congest data transmission and intercept accurate information availability^[12-15]. The deception attacks signify to undermine the integrity of transmitted information, such as replay attacks^[16-18], false data injection attack^[19-20]. Both the measurement faults and adversary attacks via the internal by hacker may contribute to the unexpected time-varying injection data in sensor network. Therefore, the resilient control should be studied to defend against the unknown false data injection attack and achieve secure operation of CPSs.

To mitigate the effects generated by the false data injection attacks, different schemes are addressed for multiple theoretical CPSs, such as strict-feedback systems, multiagent systems, networked systems. In the strict-feedback CPSs, a new type of coordinate transformation is proposed to convert the sensor attacks to the multiple time-varying state feedback gains. A novel Nussbaum function is developed in the adaptive backstepping control^[21]. For nonlinear strict-feedback systems under false injection data and unknown nonlinearities, injection data compensators via neural networks are designed and an adaptive approximation recursive event-triggered control is investigated^[22]. In time-varying multiagent systems, the random stealthy false data-injection attacks on sensor and actuator channels are modeled as the Bernoulli processes. By stochastic analysis and recursive linear matrix inequalities, the prescribed H_∞ criteria are guaranteed and the event-triggered security consensus is achieved^[23]. Considering multi-agent systems with false data injection attacks and noises, the graphical theory and Kalman filter are adopted to construct distributed state estimators. Then the mean square consensus is studied to accomplish the security mechanism^[24]. In networked systems in linear stochastic discrete form, a Kalman filter-based detection is designed to compensate for the feedback/forward channel delays and a predictive control scheme is formulated^[25]. For networked switched T-S fuzzy systems, a delay system transformation and average dwell time technique are utilized to develop event-triggering mechanism and adaptive controller^[26].

In practice CPSs, automatic voltage control or load frequency control of a power system is investigated in presence of false data injection attacks. To accomplish the automatic voltage control, the optimal stealthy attack strategy is modeled as a partial observable Markov decision process. Then, a Q-learning algorithm in nearest sequence memory is developed to learn and analogy the attack online. Finally, the kernel density estimation is conducted to detect the bad data and offset the disruptive attack impacts^[27]. In smart grids, petri nets are introduced to model the cyber-attacks, and the event trigger control is proposed to suppress the voltage fluctuation in power system^[28]. In automatic generation control to keep the grid frequency fixed at a nominal value, an optimal attack is modelled and analyzed to guide the protection of sensor data links, then efficient algorithms are provided to estimate and mitigate attack impact^[29]. A novel resilient load frequency control is proposed, where artificial neural network and Luenberger observer are combined to detect anomalies online and eliminate the adverse attack effects^[30].

The adversarial attackers supervise the measured state information furtively and send hostile deception attacks/false injection attacks depended on the state variables, which make the exactly measured state variables unavailable. Only the corrupted system states can be provided to accomplish state-feedback control design. Thus, the corrupted system dynamic is deduced tentatively. After theoretical inferences, the injected false attack information generates nonlinear system uncertainties and unknown control direction at the last step.

In the celebrated active disturbance rejection control(ADRC), extended state observers (ESOs) can estimate and compensate total disturbances such as system nonlinearities, uncertainties, and external disturbances, to improve the performance and robustness. Inspired by the above analysis,

ESOs are introduced to implement the recursive backstepping control, for strict-feedback CPSs in presence of false injection attacks in sensor networks. Specifically, a ESO is formulated to estimate the nonlinear system uncertainty term induced by false injection attacks at each step. At the last step, an extra ESO is explored owing to the unknown control direction, while Nussbaum function is exploited to achieve resilient control. The thought provides the innovation and novelty of the paper.

The paper is arranged as following: Section II elaborates problem formulation and preliminaries. An adaptive recursive control is constructed in Section III. Section IV provides the stability analysis of closed-loop system. Simulation examples are included to illustrate the effectiveness of the proposed control schemes in Section V. Finally, Section VI states concluding remarks.

II. Problem Formulation and Preliminaries

Consider the strict-feedback CPSs under false data injection attacks in sensor network, described by:

$$\begin{cases} \dot{x}_1(t) = f_1(x_1(t)) + g_1 x_2(t) \\ \dot{x}_i(t) = f_i(\bar{x}_i(t)) + g_i x_{i+1}(t) \\ \dot{x}_n(t) = f_n(\bar{x}_n(t)) + g_n u(t) \\ x_k^c(t) = x_k(t) + \eta_k(x_k(t), t) \end{cases} \quad (1)$$

where $i = 2, 3, \dots, n-1$, $k = 1, 2, \dots, n$, $\bar{x}_i(t) = [x_1(t), x_2(t), \dots, x_i(t)] \in \mathbb{R}^i$ is system state vector, $u(t) \in \mathbb{R}$ is event-triggered control to be specified later, $x_k^c(t) \in \mathbb{R}$ is the available corrupted system state, $\eta_k(x_k(t), t): (\mathbb{R}^k \times \mathbb{R}) \mapsto \mathbb{R}$ is the unknown false data injection attack term in the k^{th} sensor. The C^1 nonlinear function $f_k(\bar{x}_k(t)): \mathbb{R}^k \mapsto \mathbb{R}$ is assumed to be unknown. g_k is known positive system parameter.

Assumption 1^[21]: The false data injection attack $\eta_k(x_k(t), t)$ can be parameterized as $\eta_k(x_k(t), t) = \lambda(t)x_k(t)$, where $\lambda(t)$ is unknown time-varying gain.

Assumption 2^{[31][32]}: The unknown gain $\lambda(t)$, its first derivate $\dot{\lambda}(t)$ and second derivate $\ddot{\lambda}(t)$ are bounded, i.e., $|\lambda(t)| \leq \lambda_M$, $|\dot{\lambda}(t)| \leq \lambda_M^d$, $|\ddot{\lambda}(t)| \leq \lambda_M^{2d}$, where $\lambda_M, \lambda_M^d, \lambda_M^{2d}$ are unknown positive constants.

Assumption 3^[21]: The unknown gain $\lambda(t)$ satisfies that $1 + \lambda(t) \neq 0$, subsequently a general assumption is made that $1 + \lambda(t) > 0$.

The real system state is unavailable owing to the false data injection attack, can be denote as:

$$x_k(t) = \kappa(t)x_k^c(t) \quad (2)$$

where $\kappa(t) = 1/(1 + \lambda(t))$. From Assumption 2 and Assumption 3, the term $\kappa(t)$, its first derivate $\dot{\kappa}(t)$ and second derivate $\ddot{\kappa}(t)$ are bounded, that is, $\kappa_m \leq |\kappa(t)| \leq \kappa_M$, $|\dot{\kappa}(t)| \leq \kappa_M^d$, $|\ddot{\kappa}(t)| \leq \kappa_M^{2d}$, where $\kappa_m, \kappa_M, \kappa_M^d, \kappa_M^{2d}$ are unknown positive constants.

Assumption 4^[33]: The nonlinear real-valued continuous function $f_k(\bullet)$ and its first derivate $\dot{f}_k(\bullet)$ are available and bounded.

Def. 1^[34]: If the continuous function $N(s)$ satisfies that

$$\begin{aligned} \limsup_{k \rightarrow \pm\infty} \frac{1}{k} \int_0^k N(s) ds &= \infty \\ \liminf_{k \rightarrow \pm\infty} \frac{1}{k} \int_0^k N(s) ds &= -\infty \end{aligned} \quad (3)$$

then $N(s)$ is a Nussbaum function.

Lemma 1^[35]: $V_N(\bullet)$ and $\chi(\bullet)$ are two smooth functions on $[0, t_f)$; $V_N(t) \geq 0, \forall t \in [0, t_f)$; $N(s)$ is a Nussbaum-type function; θ_0 is a non-zero constant. If the following formula (4) holds,

$$V_N(t) \leq \int_0^t (\theta_0 N(\chi(s)) - 1) \dot{\chi}(s) ds + \mu_0, \quad \forall t \in [0, t_f) \quad (4)$$

with μ_0 is a proper constant and $\mu_1 > 0$, then $V_N(t)$, $\chi(t)$ and $\int_0^t (\theta_0 N(\chi(s)) - 1) \dot{\chi}(s) ds$ are bounded on $[0, t_f)$.

The adaptive resilient control problem tolerating sensor attack is to accomplish an adaptive control strategy, such that the strict-feedback CPSs (1) can be stabilized, and all the signals in the resulting closed-loop system remain bounded.

Notations. $\ell(\bullet)$ denote the set of continuous differentiable functions, $\|\bullet\|$ denotes the Euclid norm of $\mathbb{R}^n$.

III. Adaptive Recursive Control

Considering the false data injection attack model (2), the strict-feedback CPSs (1) can be rewritten as:

$$\begin{cases} \dot{x}_1^c = \frac{1}{\kappa} f_1(\kappa x_1^c) - \frac{\dot{\kappa}}{\kappa} x_1^c + g_1 x_2^c \\ \dot{x}_i^c = \frac{1}{\kappa} f_i(\kappa \bar{x}_i^c) - \frac{\dot{\kappa}}{\kappa} x_i^c + g_i x_{i+1}^c \\ \dot{x}_n^c = \frac{1}{\kappa} f_n(\kappa \bar{x}_n^c) - \frac{\dot{\kappa}}{\kappa} x_n^c + \frac{1}{\kappa} g_n u \end{cases} \quad (5)$$

The resilient control problem of CPSs in presence of false data injection attacks (1) can be converted into the stabilization problem of CPSs (1) subjected to lumped system uncertainties $\frac{1}{\kappa} f_i(\kappa \bar{x}_i^c) - \frac{\dot{\kappa}}{\kappa} x_i^c, i = 2, 3, \dots, n-1$ and unknown control direction $\frac{1}{\kappa} g_n$, as the false data injection attacks term $\kappa(t)$ and nonlinear function $f_i(\bar{x}_i)$ are unknown previously.

The backstepping and ADRC are adopted to implement the recursive control with the corrupted state information in the section. At each step in the recursive design process, the celebrated ADRC scheme is introduced and the extended state observer(ESO) is designed to approximate the lumped system uncertainties. At the last step, the Nussbaum function is introduced to tackle unknown control direction.

The following coordinate transformation is defined as:

$$\begin{cases} z_1(t) = x_1^c(t) \\ z_i(t) = x_i^c(t) - u_{i-1}^f(t), \quad i = 2, \dots, n \end{cases} \quad (6)$$

with $z_i(t)$ is the tracking error, $u_i^f(t)$ is the filtered signal of smooth virtual control $u_i(t)$ passing by a first-order filter:

$$\dot{u}_i^f(t) = \frac{1}{\tau} (u_i(t) - u_i^f(t)), \quad u_i^f(0) = u_i(0), i = 1, \dots, n-1 \quad (7)$$

where τ is the filter gain $0 < \tau < \min\{\frac{2}{1+g_i}, 1\}$.

The filter error is defined as:

$$e_i(t) = u_i^f(t) - u_i(t) \quad (8)$$

To facilitate the expression, the suffixes (t) are omitted in the later section.

Step 1: The dynamic of z_1 is:

$$\dot{z}_1 = \frac{1}{\kappa} f_1(\kappa x_1^c) - \frac{\dot{\kappa}}{\kappa} x_1^c + g_1(z_2 + e_1 + u_1) \quad (9)$$

A ESO is constructed to estimate the system uncertainty term $\zeta_1 = \frac{1}{\kappa} f_1(\kappa x_1^c) - \frac{\dot{\kappa}}{\kappa} x_1^c$:

$$\begin{cases} \dot{\hat{x}}_1^c = \hat{\zeta}_1 + g_1 x_2^c + \psi_{11}\left(\frac{1}{\varepsilon} \tilde{x}_1^c\right) \\ \dot{\hat{\zeta}}_1 = \frac{1}{\varepsilon} \psi_{12}\left(\frac{1}{\varepsilon} \tilde{x}_1^c\right) \end{cases} \quad (10)$$

where $\hat{x}_1^c$ and $\hat{\zeta}_1$ are estimations of corrupted system state x_1^c and lumped uncertainty ζ_1 , pertinent chosen functions $\psi_{11}(\bullet), \psi_{12}(\bullet) \in \ell(\mathbb{R}, \mathbb{R})$, ε is a small positive constant.

The notations $\tilde{x}_1^c = x_1^c - \hat{x}_1^c$ and $\tilde{\zeta}_1 = \zeta_1 - \hat{\zeta}_1$ are the estimation errors of system state and lumped uncertainty, which satisfy that:

$$\begin{cases} \dot{\tilde{x}}_1^c = \tilde{\zeta}_1 - \psi_{11}\left(\frac{1}{\varepsilon} \tilde{x}_1^c\right) \\ \dot{\tilde{\zeta}}_1 = \dot{\zeta}_1 - \frac{1}{\varepsilon} \psi_{12}\left(\frac{1}{\varepsilon} \tilde{x}_1^c\right) \end{cases} \quad (11)$$

From **Assumption 2-4**, there is a positive constant ζ_{1M}^d , such that the first derivate of lumped uncertainty $\dot{\zeta}_1$ is bounded, i.e., $|\dot{\zeta}_1| \leq \zeta_{1M}^d$. The similar conditions hold for the remaining $n-1$ subsystem.

To stabilize the z_1 -dynamic, the virtual control u_1 is defined as:

$$u_1 = \frac{1}{g_1} (-k_1 z_1 - \hat{\zeta}_1) \quad (12)$$

The Eqns.(9) yields that:

$$\dot{z}_1 = -k_1 z_1 + g_1 z_2 + g_1 e_1 + \tilde{\zeta}_1 \quad (13)$$

Step 2 $2 \leq i \leq n-1$: The dynamic of z_i is:

$$\dot{z}_i = g_i x_{i+1}^c + \zeta_i - \dot{u}_{i-1}^f = g_i (z_{i+1} + e_i + u_i) + \zeta_i - \dot{u}_{i-1}^f \quad (14)$$

where ζ_i is the lumped system uncertainty $\zeta_i \triangleq \frac{1}{\kappa} f_i(\kappa \bar{x}_i^c) - \frac{\dot{\kappa}}{\kappa} x_i^c$.

A similar ESO is constructed to estimate the lumped system uncertainty ζ_i :

$$\begin{cases} \dot{\hat{x}}_i^c = \hat{\zeta}_i + g_i x_{i+1}^c + \psi_{i1}\left(\frac{1}{\varepsilon} \tilde{x}_i^c\right) \\ \dot{\hat{\zeta}}_i = \frac{1}{\varepsilon} \psi_{i2}\left(\frac{1}{\varepsilon} \tilde{x}_i^c\right) \end{cases} \quad (15)$$

where the functions $\psi_{i1}(\bullet), \psi_{i2}(\bullet) \in \ell(\mathbb{R}, \mathbb{R})$, $\hat{x}_i^c$ and $\hat{\zeta}_i$ are estimations of x_i^c and ζ_i , $\tilde{x}_i^c = x_i^c - \hat{x}_i^c$ and $\tilde{\zeta}_i = \zeta_i - \hat{\zeta}_i$ are the estimation errors:

$$\begin{cases} \dot{\tilde{x}}_i^c = \tilde{\zeta}_i - \psi_{i1} \left(\frac{1}{\varepsilon} \tilde{x}_i^c \right) \\ \dot{\tilde{\zeta}}_i = \dot{\zeta}_i - \frac{1}{\varepsilon} \psi_{i2} \left(\frac{1}{\varepsilon} \tilde{x}_i^c \right) \end{cases} \quad (16)$$

To stabilize the z_i -dynamic, the i^{th} virtual control u_i is defined as:

$$u_i = \frac{1}{g_i} (-k_i z_i - \dot{\tilde{\zeta}}_i - g_{i-1} z_{i-1} + \dot{u}_{i-1}^f) \quad (17)$$

with k_i is the positive controller gain.

The Eqns.(14) can be deduced as:

$$\dot{z}_i = -k_i z_i - g_{i-1} z_{i-1} + g_i z_{i+1} + g_i e_i + \tilde{\zeta}_i \quad (18)$$

Define the scale estimation error vector of system state and lumped uncertainty as $\eta_i = [\eta_{i1}, \eta_{i2}]^T \in \mathbb{R}^2, i=1, 2, \dots, n-1$ and $\eta_{i1} = \frac{1}{\varepsilon} \tilde{x}_i^c, \eta_{i2} = \tilde{\zeta}_i$:

$$\begin{cases} \varepsilon \dot{\eta}_{i1} = \eta_{i2} - \psi_{i1}(\eta_{i1}) \\ \varepsilon \dot{\eta}_{i2} = \varepsilon \dot{\tilde{\zeta}}_i - \psi_{i2}(\eta_{i1}) \end{cases} \quad (19)$$

The η_i -dynamic satisfy the following **Assumption 5**.

Assumption 5. There exist the positive define, continuous differentiable functions $V_i(\eta_{i1}, \eta_{i2}), W_i(\eta_{i1}, \eta_{i2}) : \mathbb{R}^2 \mapsto \mathbb{R}$, such that:

$$\begin{aligned} \sigma_{i1} \|\eta_i\|^2 &\leq V_i(\eta_i) \leq \sigma_{i2} \|\eta_i\|^2 \\ \sigma_{i3} \|\eta_i\|^2 &\leq W_i(\eta_i) \leq \sigma_{i4} \|\eta_i\|^2 \\ \frac{\partial V_i}{\partial \eta_{i1}} (\eta_{i2} - \psi_{i1}(\eta_{i1})) - \frac{\partial V_i}{\partial \eta_{i2}} \psi_{i2}(\eta_{i1}) &\leq -W_i(\eta_i) \\ \left| \frac{\partial V_i}{\partial \eta_{i2}} \right| &\leq \mathcal{G}_i \|\eta_i\| \end{aligned} \quad (20)$$

where $\sigma_{i1}, \sigma_{i2}, \sigma_{i3}, \sigma_{i4}, \mathcal{G}_i$ are positive constants.

Step n: The dynamic of x_n^c is:

$$\dot{z}_n = \zeta_n + \frac{1}{\kappa} g_n u - \dot{u}_{n-1}^f \quad (21)$$

with ζ_n is the lumped system uncertainty $\zeta_n \triangleq \frac{1}{\kappa} f_n(\kappa \bar{x}_n^c) - \frac{\dot{\kappa}}{\kappa} x_n^c$.

Two ESOs are proposed to approximate x_n^c and ζ_n as:

$$\begin{aligned} ESO_1 : \begin{cases} \dot{l}_{1,1} = c_1(x_n^c - l_{1,1}) + l_{1,2} \\ \dot{l}_{1,2} = c_2(x_n^c - l_{1,1}) \end{cases} \\ ESO_2 : \begin{cases} \dot{l}_{2,1} = -c_1 l_{2,1} + l_{2,2} + g_n u \\ \dot{l}_{2,2} = -c_2 l_{2,1} \end{cases} \end{aligned} \quad (22)$$

with $l_{i,j}$, $i, j=1, 2$ is the state of ESOs. Define the estimation error vector as $p = [p_1, p_2]^T$ and $p_1 = x_n^c - (l_{1,1} + \frac{1}{\kappa} l_{2,1}), p_2 = \zeta_n - (l_{1,2} + \frac{1}{\kappa} l_{2,2})$, yielding that:

$$\begin{cases} \dot{p}_1 = \zeta_n + \frac{1}{\kappa} g_n u - (c_1(x_n^c - l_{1,1}) + l_{1,2} + \frac{1}{\kappa}(-c_1 l_{2,1} + l_{2,2} + g_n u)) = \zeta_n - l_{1,2} - \frac{1}{\kappa} l_{2,2} - c_1(x_n^c - l_{1,1} - \frac{1}{\kappa} l_{2,1}) \\ \quad = p_2 - c_1 p_1 \\ \dot{p}_2 = \dot{\zeta}_n - c_2(x_n^c - l_{1,1} - \frac{1}{\kappa} l_{2,1}) = \dot{\zeta}_n - c_2 p_1 \end{cases} \quad (23)$$

The p -dynamic can be expressed in vector form:

$$\dot{p} = A_0 p + \bar{\zeta}_n \quad (24)$$

with $A_0 \triangleq \begin{bmatrix} -c_1 & 1 \\ -c_2 & 0 \end{bmatrix}$, $\bar{\zeta}_n \triangleq \begin{bmatrix} 0 \\ \dot{\zeta}_n \end{bmatrix}$.

As long as $\|\bar{\zeta}_n\| = |\dot{\zeta}_n| \leq \zeta_{nM}^d$ and matrix A_0 is Hurwitz, p can convergent to the neighborhood near zero $(0, \zeta_{nM}^d / \lambda_{\min}(A_0))$ asymptotically. The estimation equation of p -dynamic can be defined as:

$$\dot{\hat{p}} = A_0 \hat{p} \quad (25)$$

Then, the n^{th} corrupted system state and lumped system uncertainty is:

$$\begin{aligned} x_n^c &= l_{1,1} + \frac{1}{\kappa} l_{2,1} + \hat{p}_1 \\ \zeta_n &= l_{1,2} + \frac{1}{\kappa} l_{2,2} + \hat{p}_2 \end{aligned} \quad (26)$$

The dynamic of z_n is:

$$\dot{z}_n = l_{1,2} + \frac{1}{\kappa} U + \hat{p}_2 - \dot{u}_{n-1}^f \quad (27)$$

where U is the reconstructed control input $U \triangleq g_n u + l_{2,2}$.

Considering the issue of false data injection attack, the control direction $\frac{1}{\kappa}$ is unknown.

Nussbaum function is utilized to construct the control input U :

$$\begin{aligned} U &= N(\xi) \bar{U} \\ \dot{\xi} &= z_n \bar{U} \\ \bar{U} &= (-k_n z_n - l_{1,2} - g_{n-1} z_{n-1} + \dot{u}_{n-1}^f) \end{aligned} \quad (28)$$

with k_n is the positive controller gain, $N(\bullet)$ is Nussbaum function.

The Eqns.(27) can be deduced as:

$$\dot{z}_n = l_{1,2} + \frac{1}{\kappa} N(\xi) \bar{U} + \hat{p}_2 - \dot{u}_{n-1}^f = -k_n z_n - g_{n-1} z_{n-1} + \hat{p}_2 + (\frac{1}{\kappa} N(\xi) - 1) \bar{U} \quad (29)$$

IV. Stability Analysis

The main result of the paper is summarized in the following theorem.

Theorem 1: Providing that *Assumption 1-5* are satisfied, consider the cyber-physical systems in strict-feedback form (1) subjected to the false data injection attacks through sensor networks and the recursive controller (28) with ESOs (10),(15),(22). Then there exist $\varepsilon_0 > 0$ such that for any $\varepsilon \in (0, \varepsilon_0)$:

- (i) The signals in the closed-loop system are semi-globally uniformly ultimately bounded(SGUUB).
- (ii) For every positive constant t_0 and $1 \leq i \leq n-1$, $\lim_{\varepsilon \rightarrow 0} |x_i^c - \hat{x}_i^c| = 0, \lim_{\varepsilon \rightarrow 0} |\zeta_i - \hat{\zeta}_i| = 0$ uniformly in $t \in [t_0, \infty)$;

$$\lim_{t \rightarrow \infty} |x_i^c - \hat{x}_i^c| \leq O(\varepsilon^2), \lim_{t \rightarrow \infty} |\zeta_i - \hat{\zeta}_i| \leq O(\varepsilon).$$

with the controller gains chosen as $k_i > \frac{1}{2}(g_i + 1), i = 1, 2, \dots, n-1, k_n > d$.

Proof. Firstly, the convergence of extended state observers (10) and (15) in the first $n-l^{\text{th}}$ subsystems is discussed.

By **Assumption 5**, the first derivate dynamic of Lyapunov function $V_i(\eta_i)$ along the trajectory (19) is:

$$\frac{dV_i(\eta_i)}{dt} = \frac{\partial V_i}{\partial \eta_{i1}}(\eta_{i2} - \psi_{i1}(\eta_{i1})) - \frac{\partial V_i}{\partial \eta_{i2}}\psi_{i2}(\eta_{i1}) + \frac{\partial V_i}{\partial \eta_{i2}}\varepsilon\dot{\zeta}_i \leq -W_i(\eta_i) + \varepsilon\zeta_{iM}^d \mathcal{G}_i \|\eta_i\| \leq -\frac{\sigma_{i3}}{\sigma_{i2}}V_i(\eta_i) + \frac{\sqrt{\sigma_{i1}}}{\sigma_{i1}}\varepsilon\zeta_{iM}^d \mathcal{G}_i \sqrt{V_i(\eta_i)} \quad (30)$$

with $|\dot{\zeta}_i| \leq \zeta_{iM}^d$.

Then we can deduce that:

$$\frac{d}{dt}\sqrt{V_i(\eta_i)} \leq -\frac{\sigma_{i3}}{2\sigma_{i2}}\sqrt{V_i(\eta_i)} + \frac{\sqrt{\sigma_{i1}}}{2\sigma_{i1}}\varepsilon\zeta_{iM}^d \mathcal{G}_i \quad (31)$$

Considering **Assumption 5**, it follows that:

$$\|\eta_i\| \leq \sqrt{\frac{V_i(\eta_i)}{\sigma_{i1}}} \leq \frac{\sqrt{\sigma_{i1}V_i(\eta_i(0))}}{\sigma_{i1}} e^{-\frac{\sigma_{i3}}{2\sigma_{i2}}t} + \frac{\varepsilon\zeta_{iM}^d \mathcal{G}_i}{2\sigma_{i1}} \int_0^t e^{-\frac{\sigma_{i3}}{2\sigma_{i2}}(t-s)} ds \quad (32)$$

Recall the definition of η_{i1}, η_{i2} , yielding that:

$$\begin{aligned} |\tilde{x}_i^c(t)| &= \varepsilon |\eta_{i1}(\frac{t}{\varepsilon})| \leq \varepsilon \|\eta_i(\frac{t}{\varepsilon})\| \leq \varepsilon \left[\frac{\sqrt{\sigma_{i1}V_i(\eta_i(0))}}{\sigma_{i1}} e^{-\frac{\sigma_{i3}t}{2\sigma_{i2}\varepsilon}} + \frac{\varepsilon\zeta_{iM}^d \mathcal{G}_i}{2\sigma_{i1}} \int_0^{\frac{t}{\varepsilon}} e^{-\frac{\sigma_{i3}}{2\sigma_{i2}}(\frac{t}{\varepsilon}-s)} ds \right] \rightarrow 0 \\ |\tilde{\zeta}_i(t)| &= |\eta_{i2}(\frac{t}{\varepsilon})| \leq \|\eta_i(\frac{t}{\varepsilon})\| \leq \left[\frac{\sqrt{\sigma_{i1}V_i(\eta_i(0))}}{\sigma_{i1}} e^{-\frac{\sigma_{i3}t}{2\sigma_{i2}\varepsilon}} + \frac{\varepsilon\zeta_{iM}^d \mathcal{G}_i}{2\sigma_{i1}} \int_0^{\frac{t}{\varepsilon}} e^{-\frac{\sigma_{i3}}{2\sigma_{i2}}(\frac{t}{\varepsilon}-s)} ds \right] \rightarrow 0 \end{aligned} \quad (33)$$

uniformly in $t \in [t_0, \infty)$ as $\varepsilon \rightarrow 0$.

Follow from Eqns.(33), the **Theorem 1(ii)** holds.

Then the boundedness of the filter error (8) is discussed. The Lyapunov function candidate is chosen as $V_e = \frac{1}{2} \sum_{i=1}^{n-1} e_i^2$, then the first derivate is:

$$\dot{V}_e = \sum_{i=1}^{n-1} e_i \dot{e}_i = \sum_{i=1}^{n-1} e_i (-\frac{1}{\tau} e_i - \dot{u}_i) \leq \sum_{i=1}^{n-1} (-\frac{1}{\tau} - \frac{1}{2}) e_i^2 + \frac{1}{2} (u_{iM}^d)^2 \quad (34)$$

with a general assumption provided that $|\dot{u}_i| \leq u_{iM}^d$.

Finally, the boundedness of extended state observers (22) in the n^{th} subsystem and the tracking error (6) is discussed.

The Lyapunov function candidate is chosen as $V = \frac{1}{2} \sum_{i=1}^n z_i^2 + \frac{1}{d} \hat{p}^T P_0 \hat{p} + \tilde{p}^T P_0 \tilde{p} + V_e$, where $P_0 A_0 + A_0^T P_0 = -I$, $\tilde{p} \triangleq p - \hat{p}$ is denoted as the estimation error of p , d is a positive constant. Then the first derivate along the trajectory (13), (18) and (29) is:

$$\begin{aligned} \dot{V} &= \sum_{i=1}^n (-k_i z_i^2) + \sum_{i=1}^{n-1} (g_i z_i e_i + z_i \tilde{\zeta}_i + e_i \dot{e}_i) + \hat{p}_2 z_n + z_n (\frac{1}{\kappa} N(\xi) - 1) \bar{U} - \frac{1}{d} \hat{p}^T \hat{p} + \dot{\tilde{p}}^T P_0 \tilde{p} + \tilde{p}^T P_0 \dot{\tilde{p}} + \dot{V}_e \\ &\leq \sum_{i=1}^{n-1} (-k_i - \frac{1}{2} g_i - \frac{1}{2}) z_i^2 + \frac{1}{2} g_i e_i^2 + \frac{1}{2} \tilde{\zeta}_i^2 - (k_n - d) z_n^2 - d(z_n - \frac{1}{2d} \hat{p}_2)^2 + z_n (\frac{1}{\kappa} N(\xi) - 1) \bar{U} - \frac{3}{4d} \hat{p}^T \hat{p} \\ &\quad - (1 - \omega) \tilde{p}^T \tilde{p} + \frac{1}{\omega} \|P_0\|^2 (\zeta_{nM}^d)^2 + \dot{V}_e \\ &\leq \sum_{i=1}^{n-1} (-k_i - \frac{1}{2} g_i - \frac{1}{2}) z_i^2 + \frac{1}{2} \tilde{\zeta}_i^2 - (\frac{1}{\tau} - \frac{1}{2} - \frac{1}{2} g_i) e_i^2 + \frac{1}{2} (u_{iM}^d)^2 - (k_n - d) z_n^2 + z_n (\frac{1}{\kappa} N(\xi) - 1) \bar{U} - \frac{3}{4d} \hat{p}^T \hat{p} \\ &\quad - (1 - \omega) \tilde{p}^T \tilde{p} + \frac{1}{\omega} \|P_0\|^2 (\zeta_{nM}^d)^2 \\ &\leq -\gamma V + (\frac{1}{\kappa} N(\xi) - 1) \bar{\xi} + \gamma_0 \end{aligned} \quad (35)$$

with $0 < \omega < 1$ is the constant to be specified, $\gamma = \min\{(2k_i - g_i - 1), (2k_n - 2d), (\frac{2}{\tau} - 1 - g_i), \frac{3}{4\lambda_{\max}(P_0)}, \frac{1-\omega}{\lambda_{\max}(P_0)}\}$, $i=1, 2, \dots, n-1$, $\gamma_0 = \sum_{i=1}^{n-1} \frac{1}{2} (u_{iM}^d)^2 + \frac{1}{\omega} (\lambda_{\max}(P_0))^2 (\zeta_{nM}^d)^2$.

Both sides of the Eqns.(35) are integrated on $[0, t]$, yielding that:

$$V \leq V(0)e^{-\gamma t} + \frac{\gamma_0}{\gamma}(1 - e^{-\gamma t}) + e^{-\gamma t} \int_0^t (\frac{1}{\kappa} N(\xi) - 1) \dot{\xi} e^{\gamma s} ds$$

By **Lemma 1**, we can deduce that the V and ξ are SGUUB. By signal chasing, the signals $z_i, \hat{p}, \tilde{p}$ are SGUUB. Recalling the definition (2)(6)(8)(28), x_i, u_i^f, u_i, u are SGUUB subsequently. All the signals in the closed-loop system are SGUUB.

The proof is completed. $\square$

V. Simulation Examples

Two simulation examples are studied to illustrate the effectiveness of the proposed control scheme to resist the false data injection in full state measurements.

Example 1: A nonlinear second-order system is considered:

$$\begin{cases} \dot{x}_1 = x_1^2 \sin(x_1) + x_2 \\ \dot{x}_2 = x_1 x_2 + x_2 \cos(x_1) + u \\ x_1^c = x_1 + (0.5 + \cos(1.2t))x_1 \\ x_2^c = x_2 + (0.5 + \sin(1.8t))x_2 \end{cases} \quad (36)$$

The initial conditions are set to $x_1(0) = 1.5, x_2(0) = -1$. The linear ESOs are utilized in Eqns.(10) and (15) as: $\psi_{11}(s) = \psi_{12}(s) = s$. The controller, ESOs and filter gains are chosen as $k_1 = 5, k_2 = 10, \varepsilon = 0.2, c_1 = 10, c_2 = 1, \tau = 0.2$.

The simulation figs are displayed in fig.1-fig.4. Fig.1 depicts the stabilization result and state trajectory of x_1, x_2 . The corrupted state x_1^c and its estimation value $\hat{x}_1^c$ are plotted in Fig.2. The ESOs states $t_{i,j}$, $i, j = 1, 2$ in Fig.3 and Fig.4 are smooth and converge to the corresponding steady-state value.

fig.1 system state trajectory

fig.2 corrupted state and its estimation value

fig.3 ESOs states $l_{1,j}$

fig.4 ESOs states $l_{2,j}$

Example 2: An IEEE 6 bus power system with three generators in Kron-reduced form is considered:

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = M_g^{-1}(L_{gl}L_{ll}^{-1}L_{lg} - L_{gg})x_1 - M_g^{-1}D_g x_2 + M_g^{-1}u \end{cases} \quad (37)$$

where $x_1, x_2 \in \mathbb{R}^3$ is the rotor angle vector and rotor frequency vector of generator, u denotes the equivalent power input, the generator inertial matrix and damping matrix are $M_g = \text{diag}\{0.125, 0.034, 0.016\} \in \mathbb{R}^{3 \times 3}$, $D_g = \text{diag}\{0.125, 0.068, 0.48\} \in \mathbb{R}^{3 \times 3}$, other physical parameters are:

$$L_{gl} = [\text{diag}\{-0.058, -0.063, -0.059\} \quad 0_{3 \times 3}] \in \mathbb{R}^{3 \times 6}, L_{ll} = \begin{bmatrix} L_{ll11} & L_{ll12} \\ L_{ll21} & L_{ll22} \end{bmatrix} \in \mathbb{R}^{6 \times 6}, L_{ll11} = \begin{bmatrix} 0 & 0 & -0.085 \\ 0 & -0.092 & 0 \\ 0 & 0 & 0.329 \end{bmatrix},$$

$$L_{ll12} = \begin{bmatrix} 0 & -0.092 & 0 \\ -0.161 & 0 & -0.072 \\ 0 & -0.17 & -0.101 \end{bmatrix}, L_{ll21} = \begin{bmatrix} -0.085 & -0.161 & 0 \\ -0.092 & 0 & -0.17 \\ 0 & -0.072 & -0.101 \end{bmatrix}, L_{ll22} = \text{diag}\{0.246, 0.262, 0.173\}$$

$$L_{lg} = \begin{bmatrix} \text{diag}\{-0.058, -0.063, -0.059\} \\ 0_{3 \times 3} \end{bmatrix} \in \mathbb{R}^{6 \times 3}, L_{gg} = \text{diag}\{0.058, 0.063, 0.059\} \in \mathbb{R}^{3 \times 3}$$

The corrupted system state dynamics are segmented as:

$$\begin{aligned} x_1^c &= \begin{cases} x_1, 0 < t < 10s \\ x_1 + (0.5 + \cos(1.2t))x_1, t > 10s \end{cases} \\ x_2^c &= \begin{cases} x_2, 0 < t < 10s \\ x_2 + (0.5 + \sin(1.8t))x_2, t > 10s \end{cases} \end{aligned} \quad (38)$$

The initial conditions are $x(0) = [0.5 \ 0.5 \ 0.5 \ 0.5 \ 0.5 \ 0.5]^T$. In Example 2, a similar linear ESOs are adopted as in Example 1. The controller, ESOs and filter gains are selected as $k_1 = 2, k_2 = 10, \varepsilon = 0.2, c_1 = 10, c_2 = 1, \tau = 0.2$.

fig.5 generator rotor angle vector trajectory

fig.6 generator rotor frequency vector trajectory

fig.7 corrupted state and its estimation vector

fig.8 ESOs state vector $l_{1,j}$

fig.9 ESOs state vector $l_{2,j}$

The results in both numerical example 1 and practical simulation 2 can validate the superiority of the proposed adaptive recursive control scheme, which can stabilize the strict-feedback CPSs and accommodate unknown injection attack in sensor networks.

VI. Conclusions

For a class of nonlinear strict-feedback cyber-physical system, the backstepping and ADRC are combined to develop a nonlinear resilient control framework to circumvent the malicious attacks through sensor networks. ESOs are constructed to compensate for the false injection data effects and unknown nonlinear dynamics via the corrupted states. The semi-globally uniformly ultimately boundedness of all the closed-loop signals can be achieved by Lyapunov analysis. Finally, the numerical examples are provided to illustrate the effectiveness of the proposed control. Further research can be extended to the resilient control problem of CPSs resisting DOS attacks and replay

attacks.

Conflict of Interest: The authors declare that they have no conflict of interest.

References

- [1]Yang Lu, Minghui Zhu. A control-theoretic perspective on cyber-physical privacy: Where data privacy meets dynamic systems. *Annual Reviews in Control*, 2019,47:423-440.
- [2]Derui Ding, Qing-Long Han, Yang Xiang, Xiaohua Ge, Xian-Ming Zhang. A survey on security control and attack detection for industrial cyber-physical systems. *Neurocomputing*, 2018, 275:1674-1683.
- [3]Magdi S. Mahmouda, Mutaz M. Hamdan, Uthman A. Baroudi. Modeling and control of Cyber-Physical Systems subject to cyber-attacks: A survey of recent advances and challenges. *Neurocomputing*, 2019,338:101-115.
- [4]Yonggui Liu,Bugong Xu,Yuehua Ding. Convergence Analysis of Cooperative Braking Control for Interconnected Vehicle Systems. *IEEE Transactions on Intelligent Transportation Systems*,2017,18(7):1894-1906.
- [5]Chen Yuanfang, Zhang, Yan, Maharjan, Sabita. Deep Learning for Secure Mobile Edge Computing in Cyber-Physical Transportation Systems. *IEEE Network*,2019, 33(4):36-41.
- [6]Shangguan, Lantian, Gopalswamy, Swaminathan. Health Monitoring for Cyber Physical Systems. *IEEE Systems Journal*,2020,14(1):1457-1467.
- [7]Elias Miranda-Vega Jesus,Flores-Fuentes Wendy, Sergiyenko Oleg. Optical cyber-physical system embedded on an FPGA for 3D measurement in structural health monitoring tasks.*Microprocessors and Microsystems*, 2018,56:121-133.
- [8]Domain Hildebrandt Constantin, Koecher Aljosha, Kuestner Christof. Ontology Building for Cyber-Physical Systems: Application in the Manufacturing. *IEEE Transactions on Automation Science and Engineering*, 2020,17(3): 1266-1282.
- [9]Nannapaneni Saideep,Mahadevan Sankaran, Dubey Abhishek.Online monitoring and control of a cyber-physical manufacturing process under uncertainty. *Journal of Intelligent Manufacturing*,2020, DOI: 10.1007/s10845-020-01609-7.
- [10]Zhang Meng, Shen Chao,He Ning, Han Sicong, Li Qi, Wang Qian, Guan, XiaoHong. False data injection attacks against smart grid state estimation: Construction, detection and defense. *Science China-Technological Sciences*,2019,62(12):2077-2087.
- [11]Abdallah Ahmed, Feron Eric M., Hellestrand Graham. Hardware/Software Codesign of Aerospace and Automotive Systems.*Proceedings of the IEEE*,2010,98(4): 584-602.
- [12]Zhu Yanzheng,Zheng Wei Xing. Observer-Based Control for Cyber-Physical Systems with Periodic DoS Attacks via a Cyclic Switching Strategy. *IEEE Transactions on Automatic Control*,2020, 65(8):3714-3721.
- [13]Sun Qi,Zhang Kunwu,Shi Yang. Resilient Model Predictive Control of Cyber-Physical Systems under DoS Attacks. *IEEE Transactions on Industrial Informatics*,2020,16(7):4920-4927.
- [14]Mahmoud Magdi S., Hamdan Mutaz M.,Baroudi Uthman A. Secure control of cyber physical systems subject to stochastic distributed DoS and deception attacks.*International Journal of Systems Science*,2020,51(9):1653-1668.
- [15]Tian Jiwei,Wang Buhong,Li Tengyao. Coordinated cyber-physical attacks considering DoS attacks in power systems.*International Journal of Robust and Nonlinear Control*,2020,30(11): 4345-4358.
- [16]Su Lei,Ye Dan,Zhao Xingang. Static output feedback secure control for cyber-physical systems based on multisensor scheme against replay attacks. *International Journal of Robust and Nonlinear Control*,2020,30(18) :8313-8326 .

- [17]Huang Jiangshuai,Zhao Ling,Wang Qing-Guo.Adaptive control of a class of strict feedback nonlinear systems under replay attacks.*ISA Transactions*, 2020,107:134-142.
- [18]Sabina Sanchez Helem,Rotondo Damiano,Escobet Teresa. Detection of replay attacks in cyber-physical systems using a frequency-based signature. *Journal of the Franklin Institute-Engineering and Applied Mathematics*, 2019,356(5):2798-2824.
- [19]Chattopadhyay Arpan, Mitra, Urbashi. Security Against False Data-Injection Attack in Cyber-Physical Systems.*IEEE Transactions on Control of Network Systems*, 2020, 7(2):1015-1027.
- [20]Drayer Elisabeth,Routtenberg Tirza. Detection of False Data Injection Attacks in Smart Grids Based on Graph Signal Processing. *IEEE Systems Journal*,2020,14(2):1886-1896.
- [21]Xiuxiu Ren, Guanghong Yang. Adaptive control for nonlinear cyber-physical systems under false data injection attacks through sensor networks. *International Journal of Robust and Nonlinear Control*,2020,30:65-79.
- [22]Yoo Sung Jin.Approximation-Based Event-Triggered Control Against Unknown Injection Data in Full States and Actuator of Uncertain Lower-Triangular Nonlinear Systems. *IEEE ACCESS*,2020,8:101747-101757.
- [23]Panshuo Li, Hongyi Li, Renquan Lu. Event-Triggered Consensus Control for Multi-Agent Systems Against False Data-Injection Attacks. *IEEE Transactions on Cybernetics*, 2020,50(5):1856-1866.
- [24]Zhiqiang Zuo, Xiong Cao, Yijing Wang. Security control of multi-agent systems under false data injection attacks. *Neurocomputing*,2020, 404: 240-246.
- [25]Zhonghua Pang, Guoping Liu, Donghua Zhou, Fangyuan Hou, Dehui Sun. Two-Channel False Data Injection Attacks Against Output Tracking Control of Networked Systems. *IEEE Transaction on Industrial Electronics*, 2016,63(5):3242-3251.
- [26]Yiwen Qi, Shuo Yuan, Xin Wang. Adaptive Event-triggered Control for Networked Switched T-S Fuzzy Systems Subject to False Data Injection Attacks. *International Journal of Control, Automation and Systems*, 2020, 18(10):2580-2588.
- [27]Ying Chen, Shaowei Huang, Feng Liu, Zhisheng Wang, Xinwei Sun. Evaluation of Reinforcement Learning-Based False Data Injection Attack to Automatic Voltage Control. *IEEE Transactions on Smart Grid*, 2019,10(2):2158-2169.
- [28]Rong Fu, Yue Xu, Yi Tang, Qi Wang. Petri net-based voltage control strategy under false data injection attack. *Transactions of the Institute of Measurement and Control*, 2020,42(14): 2622-2631.
- [29]Rui Tan, Hoang Hai Nguyen, Eddy. Y. S. Foo, David K. Y. Yau, Zbigniew Kalbarczyk, Ravishankar K. Iyer, Hoay Beng Gooi. Modeling and Mitigating Impact of False Data Injection Attacks on Automatic Generation Control. *IEEE Transactions on Information Forensics and Security*,2017, 12(7): 1609-1624.
- [30]Alireza Abbaspour, Arman Sargolzaei, Parisa Forouzaneshad, Kang K. Yen, Arif I. Sarwat. Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks. *IEEE Transactions on Industrial Electronics*,2020,67(9):7951-7962.
- [31]Jin Xu, Haddad Wassim M, Yucelen Tansel. An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems. *IEEE Transactions on Automatic Control*, 2017, 62(11): 6058-6064.
- [32]Liwei An, Guang-Hong Yang. Improved adaptive resilient control against sensor and actuator attacks. *Information Sciences*, 2018, 423: 145-156.
- [33]Qiang Gao, Yuehui Ji, Hailiang Zhou,Junfang Li. Adaptive homo-backstepping tracking control for strict-feedback systems in presence of unknown dead-zones. *International Journal of Adaptive Control & Signal Processing*,2017,31(8):1101-1110.
- [34]Qingling Wang,Changyin Sun. Adaptive Consensus of Multiagent Systems with Unknown High-Frequency Gain Signs Under Directed Graphs. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*,2020, 50(6):2181-2186.

[35]Kai Zhao, Yongduan Song,Tiedong Ma,Liu He. Prescribed Performance Control of Uncertain Euler-Lagrange Systems Subject to Full-State Constraints. *IEEE Transactions on Neural Networks and Learning Systems*,2018,29(8):3478-3489.

Figures

Figure 1

system state trajectory

Figure 2

corrupted state and its estimation value

Figure 3

ESOs states 2, j

Figure 4

ESOs states $l_{2,j}$

Figure 5

generator rotor angle vector trajectory

Figure 6

generator rotor frequency vector trajectory

Figure 7

corrupted state and its estimation vector

Figure 8

ESOs state vector $l_{1,j}$

Figure 9

ESOs state vector $l_{2,j}$