Robust Intrusion Detection for Resilience Enhancement of Industrial Control Systems: An Extended State Observer Approach

Ahmad, Saif; Ahmed, Hafiz

2022 IEEE Texas Power and Energy Conference (TPEC)

DOI:
https://doi.org/10.1109/TPEC54980.2022.9750751

Published: 14/04/2022

Robust Intrusion Detection for Resilience Enhancement of Industrial Control Systems: An Extended State Observer Approach

Saif Ahmad
Department of Electrical Engineering
Indian Institute of Technology Patna
Patna, India
E-mail: saifiitp16@gmail.com

Hafiz Ahmed
Nuclear Futures Institute
Bangor University
Bangor LL57 1UT, United Kingdom
E-mail: hafiz.h.ahmed@ieee.org

***Abstract*—We address the problem of attack signal estimation in industrial control systems that are subjected to actuator false data injection attack (FDIA) and where the sensor measurements are corrupted by non-negligible high-frequency measurement noise. The actuator FDIA signal is categorized as disturbance to be estimated and subsequently compensated, based on the concept of extended state observer (ESO). We investigate the efficacy of two alternatives to conventional ESO namely, cascade ESO (CESO) and low-power higher-order ESO (LHESO), that guarantee improved estimation performance in case of noisy measurement data as well as time-varying attack signals. Simulation results under different types of FDIAs demonstrate the advantages of designed schemes in comparison to conventional linear and nonlinear ESOs, using network motion control system as an illustrative example.**

***Index Terms*—actuator false data injection attack, industrial control system, extended state observer, measurement noise.**

I. Introduction

Technological advancements in the filed of digital communication have resulted in rapid adoption of networked control systems (NCSs) in the industrial setting due to various advantages such as increased flexibility in architecture, lower installation cost, easier maintenance and improved reliability, compared to a conventional control systems [1], [2]. NCSs are characterized by remote sensors located near the physical system which collect and transmit data to control systems over a communication network. However, this interaction between the physical and cyber (communication) layer also gives rise to security issues as the system becomes susceptible to malicious cyber attacks at the sensor or actuator side and carries the risk of damaging the control system [3]–[6]. Over the years, an increasing number of cyber attacks on industrial control systems are being witnessed due to a proliferation of NCSs in the industrial setting, with over 16000 attacks reported in 2013 alone [3]. Intrusion detection and design of attack resilient cyber-physical industrial control systems is therefore of paramount importance to ensure safe and reliable operation of NCSs [7]–[11].

A number of attack detection, isolation, estimation and control methods have been investigated in [3], [12]–[17]. References [3], [12] present a detailed survey on intrusion detection and recent advancements on the security issue in industrial cyber-physical systems along with the advantages and limitations of different techniques. A distributed nonlinear observer relying on higher-order sliding mode structure was constructed in [13] to estimate the system states along with unknown constant power load in a DC micro-grid scenario considering FDIA on the sensors. In [14], a bank of unknown input observers (UIO) were constructed for estimation of system states as well as the attack signal without using the input signals. An extended state observer (ESO) based approach was investigated for estimation of actuator FDIA in [15] in the context of a networked motion control platform where the attack signal was categorised as disturbance. It is to be noted that observer based estimation techniques studied in [13]–[15] are susceptible to high-frequency measurement noise that gets added during data collection. Furthermore, high-gain nature of the observers employed in [13], [15] give rise to numerical issue during practical implementation on fixed point digital signal processors due to finite word length.

Motivated by the aforementioned facts, we introduce two alternatives to conventional ESO, namely cascade ESO (CESO) [18], [19] and low-power higher-order ESO (LHESO) [20], that offer a promising solution to the problems associated with high-gain observers and analyze their effectiveness in the context of intrusion detection and attack signal estimation in a cyber-security setting considering the case of a networked motion control platform, similar to [15]. The present approach relies on attack signal estimation based on the difference between expected and actual system output under a specified control signal. An FDIA on the actuator side is considered in which the malicious data is added to the control signal during transmission over the communication network. However, unlike [15], we also consider the effect of high-

H. Ahmed is funded through the Sêr Cymru programme by the Welsh European Funding Office (WEFO) under the European Regional Development Fund (ERDF).

978-1-6654-7902-8/22/$31.00 ©2022 IEEE

frequency measurement noise that is often inevitable in sensor-based data acquisition. In particular, we show that the ability of CESO and LHESO to accurately estimate time-varying signals makes them a better alternative to conventional ESO. Furthermore, the low-power structure of LHESO limits the maximum observer gain to be implemented to 'two' which in turn takes care of the numerical issue associated with the practical implementation in a digital setting [21], [22]. We also highlight a major limitation of nonlinear ESO (NESO) in terms of oscillations around the steady state operating point which happens due to over-amplification of measurement noise. In addition, an attack decoupling control law is used to mitigate the effect of FDIA and make the industrial control system resilient to cyber attacks.

Remaining sections in this paper are organised as follows: Section II deals with the problem formulation considering actuator FDIA on a networked motion control system. Conventional linear and nonlinear ESOs are briefly revisited in Section III in the context of attack signal estimation. Section IV introduces two noise suppressing ESOs, i.e. CESO and LHESO, for attack signal estimation and highlights structural properties that result in superior estimation performance. Numerical study using Simulink/MATLAB environment is carried out in Section V to highlight the effectiveness of the designed schemes. The papers ends in Section VI with a summary of conclusions.

II. Problem Formulation

In this paper, we consider a second order networked motion control platform studied in [15] and expressed as follows:

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + bu \\ y_m &= x_1 + \nu, \end{cases} \tag{1}$$

where x_1, x_2 denote the position and speed of the motor, respectively and y_m is the sensed value of positions which is acted upon by an additive high-frequency measurement noise signal denoted by ν. A direct structure is considered for the networked control system which comprises a controller and a remote unit connected via a communication channel [1]. The remote unit further contains a physical plant i.e. servo motor, actuator and sensor for position feedback.

We consider a scenario where the system defined in (1) is subjected to a cyber attack at the actuator side, as shown in Fig. 1, where the attack signal is denoted by Δu. System (1) under actuator FDIA can be expressed as

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + b[u + \Delta u] \\ &= -ax_2 + bu + \vartheta \\ y_m &= x_1 + \nu, \end{cases} \tag{2}$$

where $\vartheta = b\Delta u$ denotes the net effect of attack signal on the dynamics of motion control platform.

Considering that the system model in (1) is accurate, the attack signal (Δu) can be estimated by using the concept of extended state observer where the unknown FDIA signal is categorised as additive disturbance term. Including ϑ in the state space model, the augmented dynamics for (2) is obtained as

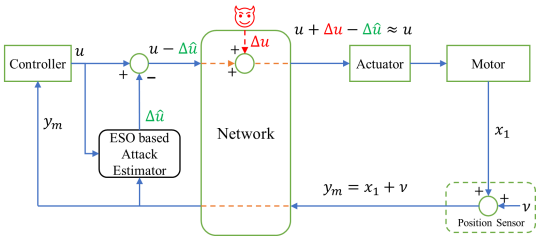

Fig. 1: Block diagram of ESO based attack resilient networked motion control platform.

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + \vartheta + bu \\ \dot{\vartheta} &= h \\ y_m &= x_1 + \nu, \end{cases} \tag{3}$$

where h denotes the derivative of ϑ.

III. Conventional Extended State Observers

In order to estimate the system states x_1, x_2 as well as the disturbance ϑ, an extended state observer is designed for the system defined in (3) and following assumptions are made to ensure the stability of ESO:

Assumption 1: Derivative of ϑ i.e. $h = \dot{\vartheta}$ is bounded in the manner $|h| \leq \mu_1$ [18].

Assumption 2: Measurement noise ν is bounded and the bound is given by $|\nu| \leq \mu_2$ [19].

A nonlinear extended state observer (NESO) is designed for (3) following the general design approach given in [23] which gives

$$\begin{cases} e_1 &= y_m - \hat{x}_1 \\ \dot{\hat{x}}_1 &= \hat{x}_2 + \beta_1 \cdot \varsigma_1(e_1) \\ \dot{\hat{x}}_2 &= -a\hat{x}_2 + \hat{\vartheta} + bu + \beta_2 \cdot \varsigma_2(e_1) \\ \dot{\hat{\vartheta}} &= \beta_3 \cdot \varsigma_3(e_1), \end{cases} \tag{4}$$

where β_1, β_2, β_3 denote observer gains and $\varsigma_i(e_1)$ is the nonlinear error function which is expressed as

$$\varsigma_i(e_1) = fal(e_1, \alpha_i, \delta) = \begin{cases} \dfrac{e_1}{\delta^{1-\alpha_i}} & |e_1| \leq \delta \\ |e_1|^{\alpha_i} sign(e_1) & |e_1| > \delta, \end{cases} \tag{5}$$

where δ is the threshold value. However, the NESO is difficult to analyse and tune due to its nonlinear nature and large number of tuning parameters. Furthermore, the small error large gain nature of the $fal(\cdot)$ function [24] results in significant noise amplification around steady state and contaminates the attack signal estimate.

In order to have a simpler implementation as well as tuning, a linear ESO (LESO) was proposed in [25] where the nonlinear function ς_i is replaced by e_1. Furthermore, the observer gains

are parameterized in terms of an observer bandwidth denoted by ω_o such that $\beta_i = \epsilon_i \omega_o^i$ where ϵ_i is a positive constant. However, high-gain nature of LESO also results in noise amplification in the obtained estimates as evidenced by the following estimation error bound obtained for a third order ESO [26]:

$$\begin{aligned} \lim_{t\to\infty} \|\tilde{\boldsymbol{x}}\| &\leq \kappa_1 |h| \omega_o^{-1} + \kappa_2 |\nu| \omega_o^2 \\ &\leq \kappa_1 \mu_1 \omega_o^{-1} + \kappa_2 \mu_2 \omega_o^2, \end{aligned} \tag{6}$$

for some $\omega_o \geq \omega_o^*$, where κ_1, κ_2 are some positive constants, $\|\tilde{\boldsymbol{x}}\| := \sqrt{\tilde{\boldsymbol{x}}^T \tilde{\boldsymbol{x}}}$ denotes the Euclidean norm of $\tilde{\boldsymbol{x}} := \boldsymbol{x} - \hat{\boldsymbol{x}}$, $\boldsymbol{x} := [x_1, x_2, \vartheta]^T$ and $\hat{\boldsymbol{x}} := [\hat{x}_1, \hat{x}_2, \hat{\vartheta}]^T$. The aforementioned inequality in (6) makes it clear that an increase in ω_o attenuates the effect of disturbance (h) by $\mathcal{O}(\omega_o^{-1})$ on the estimation error, however, the effect of measurement noise (ν) is amplified by $\mathcal{O}(\omega_o^2)$. This relation in turn forces a compromise between fast and accurate disturbance estimation and noise contamination of the estimates, while selecting the observer bandwidth. In addition, escalation of observer gains to ω_o^{n+1}, where n is the system order, gives rise to numerical issue during practical implementation on fixed-point digital signal processors [26]. These problems are addressed in the following sections by introducing alternatives to the conventional ESO structure.

IV. Noise Suppressing Extended State Observers

A. Cascade Extended State Observer

Cascade ESO [18], [19], attempts to overcome the noise amplification issue through virtual decomposition of the total disturbance into N number of components and then estimating each component via a set of N cascaded ESO where the output of ESO in each level acts as a reference for subsequent level. In doing so, the noise sensitivity of the final set of estimates obtained from CESO is improved due to filtering at each level. In this paper, a two level CESO is designed for system defined in (3), using the following expression:

$$\Sigma_1 := \begin{cases} \dot{\hat{x}}_{1,1} &= \hat{x}_{1,2} + l_{1,1}(y_m - \hat{x}_{1,1}) \\ \dot{\hat{x}}_{1,2} &= -a\hat{x}_{1,2} + \hat{\hat{\vartheta}}_1 + bu + l_{1,2}(y_m - \hat{x}_{1,1}) \\ \dot{\hat{\vartheta}}_1 &= l_{1,3}(y_m - \hat{x}_{1,1}), \end{cases}$$

$$\Sigma_2 := \begin{cases} \dot{\hat{x}}_{2,1} &= \hat{x}_{2,2} + l_{2,1}(\hat{x}_{1,1} - \hat{x}_{2,1}) \\ \dot{\hat{x}}_{2,2} &= -a\hat{x}_{2,2} + \hat{\hat{\vartheta}}_1 + \hat{\hat{\vartheta}}_2 + bu + l_{2,2}(\hat{x}_{1,1} - \hat{x}_{2,1}) \\ \dot{\hat{\vartheta}}_2 &= l_{2,3}(\hat{x}_{1,1} - \hat{x}_{2,1}), \end{cases} \tag{7}$$

where $l_{i,j}, i = \{1,2\}, j = \{1,2,3\}$, denote the observer gains, and $\hat{x}_{1,1}$ acts as a reference signal for Σ_2. The estimate of attack signal is obtained as $\hat{\vartheta} = \hat{\hat{\vartheta}}_1 + \hat{\hat{\vartheta}}_2$ while $\hat{x}_{2,1}, \hat{x}_{2,2}$ are the final state estimates which can be used in feedback control design. The expression for estimation error bound is similar to (6) and can be obtained following the approach highlighted in [18], [19].

Similar to LESO, the estimates of Σ_1 are directly affected by measurement noise and have a relative degree of unity which is the primary reason behind poor noise suppression. However, cascade ESO attempts to overcome this limitation in Σ_1 by selecting a lower observer bandwidth compared to LESO, hence, the noise content in $\hat{\hat{\vartheta}}_1$ is relatively low. Therefore, CESO results in improved noise suppression compared to LESO despite having the same relative degree between $\tilde{\vartheta} := \vartheta - \hat{\vartheta}$ and ν, i.e., unity [20]. However, CESO still suffers from the numerical implementation issue as the observer gains escalate to $\mathcal{O}(\omega_{oi}^{n+1}), i = \{1,2\}$.

Remark 1: An interesting feature of CESO that relies on virtual decomposition of disturbance is that it naturally embeds a higher-order ESO (HESO) or generalized proportional integral observer (GPIO) [27] type property into the resulting structure, i.e., CESO is able to accurately estimate ramp-type attack signals where $\ddot{\vartheta} = 0$ despite being designed based on the assumption that ϑ is constant in steady-state. However, the output estimate $(\hat{x}_{2,1})$ is not accurate in the time-varying case and results in a steady-state error if it is used in feedback control design.

B. Low-power Higher-order Extended State Observer

In order to overcome both the issues associated with high-gain ESO, i.e., noise amplification as well as numerical implementation, a low-power higher-order ESO is designed for (2) using the structure introduced in [26]. In this case, the disturbance is assumed to be time varying such that $\dddot{\vartheta} = 0$, which gives

$$\vartheta_1 = \vartheta, \dot{\vartheta}_1 = \vartheta_2, \dot{\vartheta}_2 = 0, \tag{8}$$

and is included in (2) to obtain the following augmented model:

$$\begin{cases} \dot{x}_1 &= x_2 \\ \dot{x}_2 &= -ax_2 + \vartheta + bu \\ \dot{\vartheta}_1 &= \vartheta_2 \\ \dot{\vartheta}_2 &= g, \\ y_m &= x_1 + \nu, \end{cases} \tag{9}$$

where g is second derivative of the non-zero residual term that does not match the assumed disturbance form in (8). Following assumption is made on the disturbance ϑ in order to ensure the input-to-state stability of LHESO:

Assumption 3: Second derivative of attack signal given by $\ddot{\vartheta} = g$ is bounded in the sense $|g| \leq \mu_3$.

An LHESO is designed for the system defined in (9) having two state augmentations, using the following expression:

$$\Pi_1 := \begin{cases} \dot{\hat{x}}_1 &= \hat{\hat{x}}_2 + \gamma_1 \omega_o (y_m - \hat{x}_1) \\ \dot{\hat{x}}_2 &= -a\hat{\hat{x}}_2 + \hat{\hat{\vartheta}}_1 + bu + \bar{\gamma}_1 \omega_o^2 (y_m - \hat{x}_1), \end{cases}$$

$$\Pi_2 := \begin{cases} \dot{\hat{x}}_2 &= -a\hat{x}_2 + \hat{\hat{\vartheta}}_1 + bu + \gamma_2 \omega_o (\hat{\hat{x}}_2 - \hat{x}_2) \\ \dot{\hat{\vartheta}}_1 &= \hat{\hat{\vartheta}}_2 + \bar{\gamma}_2 \omega_o^2 (\hat{\hat{x}}_2 - \hat{x}_2), \end{cases} \tag{10}$$

$$\Pi_3 := \begin{cases} \dot{\hat{\vartheta}}_1 &= \hat{\hat{\vartheta}}_2 + \gamma_3 \omega_o (\hat{\hat{\vartheta}}_1 - \hat{\vartheta}_1) \\ \dot{\hat{\vartheta}}_2 &= \bar{\gamma}_3 \omega_o^2 (\hat{\hat{\vartheta}}_1 - \hat{\vartheta}_1), \end{cases}$$

where $\hat{\bar{x}}_2, \hat{\bar{\vartheta}}_1$ act as reference signal for sub-blocks Π_2, Π_3 and $\gamma_i, \bar{\gamma}_i, (i = 1 \text{ to } 3)$ denote observer parameters. The upper bound for estimation error can easily be obtained based on the approach given in [26] and results in the following expression:

$$\begin{aligned} \lim_{t\to\infty} \|\tilde{\boldsymbol{\chi}}\| &\leq \kappa_3 |g| \omega_o^{-1} + \kappa_4 |\nu| \omega_o^3 \\ &\leq \kappa_3 \mu_3 \omega_o^{-1} + \kappa_4 \mu_2 \omega_o^3, \end{aligned} \tag{11}$$

for some $\omega_o \geq \omega_o^*$, where κ_3, κ_4 are some positive constants and $\tilde{\boldsymbol{\chi}} = [x_1, x_2, x_2, \vartheta_1, \vartheta_1, \vartheta_2]^T - [\hat{x}_1, \hat{\bar{x}}_2, \hat{x}_2, \hat{\bar{\vartheta}}_1, \hat{\vartheta}_1, \hat{\bar{\vartheta}}_2]^T$. The aforementioned inequality presents a similar compromise between disturbance rejection and noise attenuation and a straightforward comparison of the noise dependent terms in the inequalities (6) and (11) might indicate that noise amplification is more prominent in LHESO i.e. $\mathcal{O}(\omega_o^3)$, due to the inclusion of an extra augmented state. However, the bounds obtained in terms of measurement noise in both the inequalities is conservative in the sense that the frequency content of the noise signal is not taken into consideration. Particularly for $\tilde{\vartheta}$, it can be shown using frequency domain analysis that the relative degree with respect to measurement noise is unity in case of LESO as well as CESO and 3 in case of LHESO [26]. Therefore, LHESO results in better noise suppression in the high frequency range compared to LESO and CESO.

Remark 2: Design of LHESO based on the disturbance model in (8) is in contrast to the assumption in LESO and NESO that the disturbance is constant in steady state and hence, results in better estimation of time-varying attack signals. In particular, LHESO results in the asymptotic convergence of estimation error to zero for ramp attack signals, in the absence of measurement noise as is evident from (11).

V. Numerical Analysis

Numerical simulations were performed in Simulink/MATLAB environment using a fixed step-size of 0.5 ms and ode4 Runge-Kutta solver. In order to simulate the effect of sensor noise ν, a high frequency noise signal was generated by passing a band-limited white noise having noise power 10^7 and maximum frequency content of 100 Hz, through an 8^{th} order high-pass Butterworth filter having a pass-band edge frequency of $f_H = 150\pi \ rad/s$. Parameters of the servo motor were selected as $a = 113.72$ and $b = 10.72$ based on [15]. NESO and LESO parameters were also kept same as [15] while CESO and LHESO parameters were selected using a similar approach with the same bandwidths, in order to have a fair comparison. The estimator parameters used in the present study are listed in Table I. It is to be noted that the observer parameters selected for LESO, CESO, and LHESO in Table I do not place the observer poles at $-\omega_o$ due to the deviation of considered model from pure integrating structure, however, the resulting structure is stable nonetheless as the poles are located in the left half of the s-plane. Following type of attack signals are considered for evaluating the efficacy of the designed estimators:

S1: ***Bias Attack*** is characterized by a constant attack signal where the adversary adds a constant value (ρ_1) to the control signal in the attack duration and is given by

$$\vartheta(t) = \begin{cases} \rho_1, & t \in (t_i, t_f) \\ 0, & \text{otherwise.} \end{cases} \tag{12}$$

The following two bias attacks are considered in the present study: **S1(a)** - $\rho_1 = 5$ for $t \in (1, 3)s$ and **S1(b)** - $\rho_1 = 10$ for $t \in (1, 1.05)s$. If the time duration of this attack is reduced and magnitude is increased so as to maximize the damage, it becomes an impulse attack similar to S1(b).

S2: ***Ramp Attack*** is represented by a continuously increasing signal that rises with a constant slope (ρ_2) and is expressed as

$$\vartheta(t) = \begin{cases} \rho_2 \cdot (t - t_i), & t \in (t_i, t_f) \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

A slope of 30 units per second is used to simulate the effect of ramp type attack signal in the interval $t \in (1, 3)s$.

S3: ***Geometric Attack*** starts by slowly drifting the control signal from its actual value and maximizes the damage towards the end of the attack. It is given by the following expression:

$$\vartheta(t) = \begin{cases} \rho_3 \cdot \rho_4^{(t-t_i)}, & t \in (t_i, t_f) \\ 0, & \text{otherwise,} \end{cases} \tag{14}$$

where $\rho_3 = 2, \ \rho_4 = 5, \ t_i = 1s$ and $t_f = 3s$ are selected for simulation study.

S4: ***Sinusoidal Attack*** is represented using the following expression:

$$\vartheta(t) = \begin{cases} \rho_5 \sin\left(2\pi f (t - t_i)\right), & t \in (t_i, t_f) \\ 0, & \text{otherwise,} \end{cases} \tag{15}$$

where $\rho_5, \ f$ denote the amplitude, frequency and were selected as $\rho_5 = 20, \ f = 0.05, 0.5, 1$ Hz, to evaluate the estimation performance of different ESOs.

Simulation results for attack scenarios **S1** to **S4** are shown in Fig. 2. It is observed that LHESO and CESO are able to ensure better estimation accuracy despite the noisy measurement. Particularly in case of time-varying attack signals considered in **S2**, **S3** and **S4**, LHESO and CESO result in significantly lower estimation error compared to LESO and NESO, with LHESO being more accurate (lower peak-to-peak error amplitude in **S4** and smaller error value in **S3**) and having lower noise content among the two due to a higher relative degree (3 as opposed to 1 in case of CESO). Furthermore, large oscillations can be observed in case of NESO which is due to the small error high gain feature implemented via $fal(\cdot)$ function and leads to the over-amplification of measurement noise.

A. Actuator FDIA Decoupling

The estimate of attack signal can be used in combination with feedback control law to cancel the effect of FDIA on the networked motion control platform. Assuming u as the

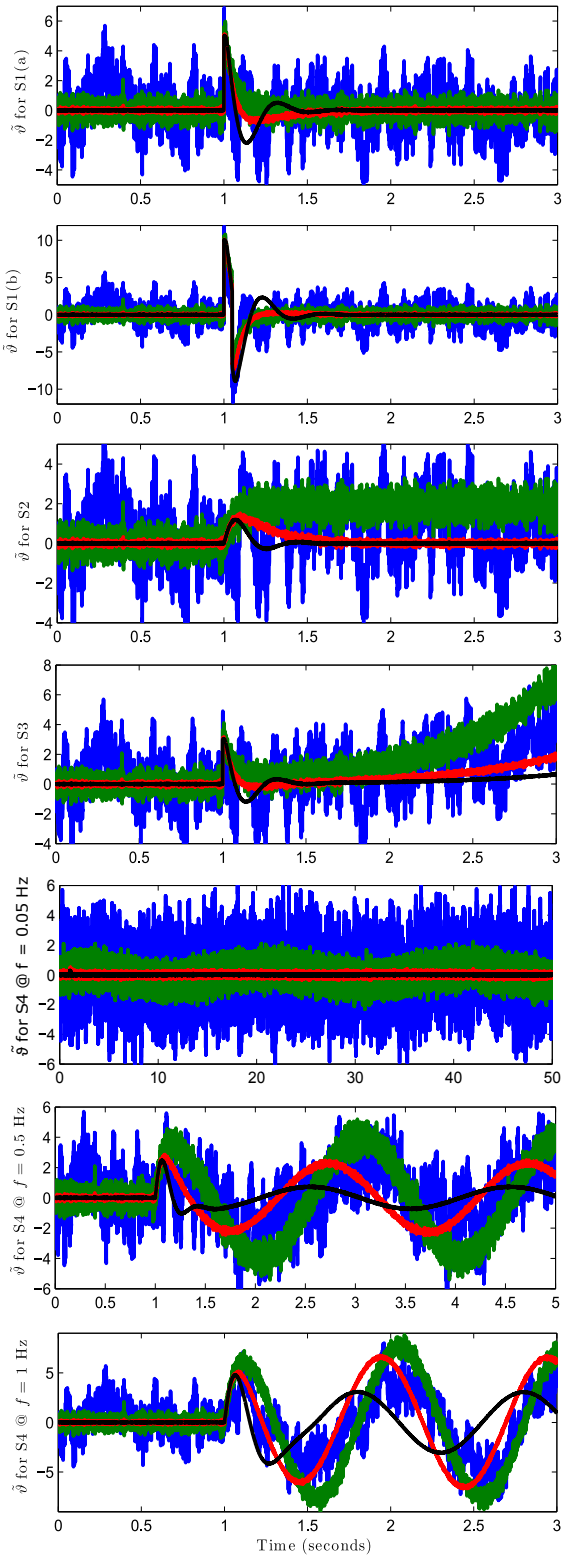

Fig. 2: Estimation error plots $\tilde{\vartheta}$ for different types of attack signals. (Legend: blue-NESO, green-LESO, red-CESO, black-LHESO)

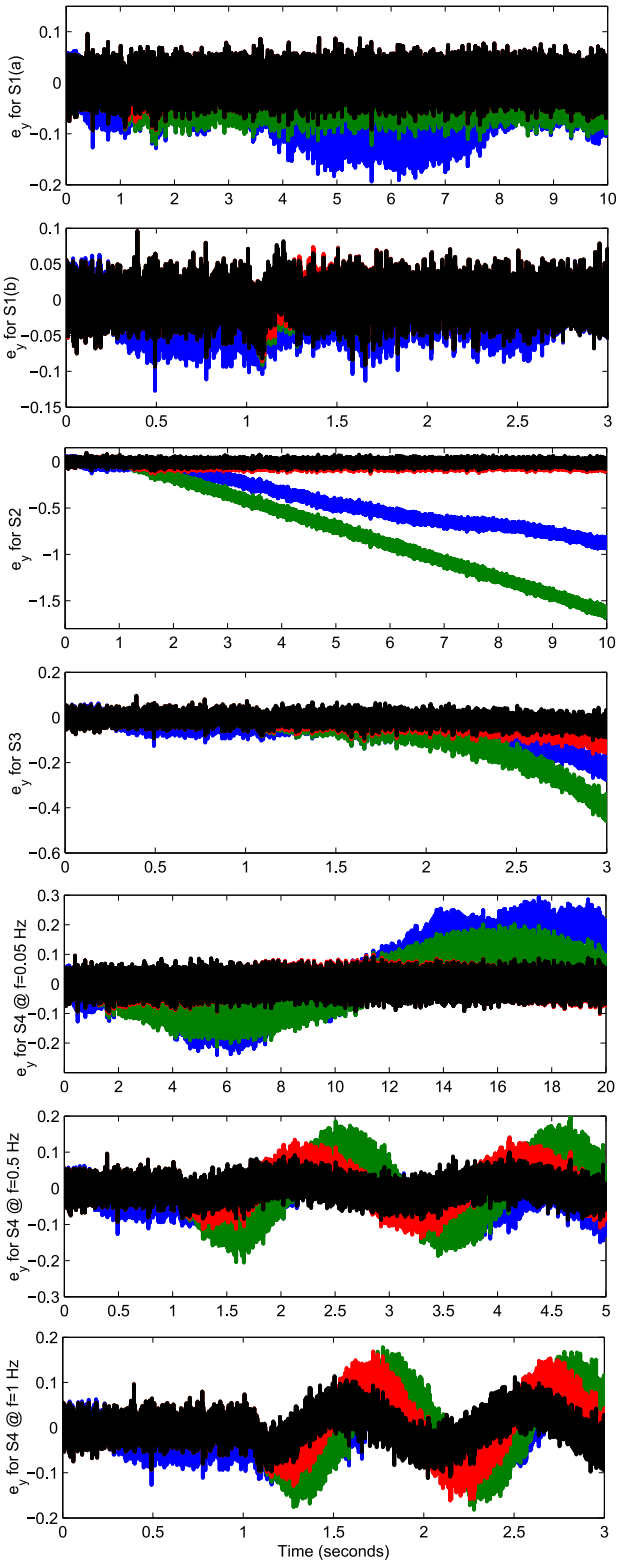

Fig. 3: Plot of output error e_y under FDIA decoupling control law (16), for different types of attack signals. (Legend: blue-NESO, green-LESO, red-CESO, black-LHESO)

TABLE I: Estimator parameters used in the numerical study

	Estimator Parameters
NESO	$\beta_1 = 400, \beta_2 = 2000, \beta_3 = 89900, \delta = 0.01, \alpha_i = 1/2^{i-1}$
LESO	$\omega_o = 100rad/s, \beta_1 = 3\omega_o, \beta_2 = 3\omega_o^2, \beta_3 = \omega_o^3$
CESO	$\omega_{o1} = 50rad/s,\ \omega_{o2} = 100rad/s,$ $l_{i,1} = 3\omega_{oi}, l_{i,2} = 3\omega_{oi}^2, l_{i,3} = \omega_{oi}^3, i = \{1, 2\}$
LHESO	$\omega_o = 100rad/s, \bar{\gamma}_1 = 3, \bar{\gamma}_2 = 1, \bar{\gamma}_3 = 1/3,$ $\gamma_1 = \gamma_2 = \gamma_3 = 2$

feedback control signal, an attack decoupling control law of the form

$$\bar{u} = -\frac{\hat{\vartheta}}{b} + u = -\Delta\hat{u} + u, \tag{16}$$

can be used to negate the effect of attack signal on the motion control platform as shown in Fig. 1. In order to analyse the effectiveness of the designed schemes in negating the effect of FDIA on the networked motion control platform, we apply the attack decoupling control law given in (16) and subtract the output of the affected system from the output of a system that is not under attack. The error between desired output and actual output under the effect of actuator FDIA and sensor noise is denoted by e_y and gives an idea regarding the attack resilience of the proposed schemes. Simulation plots obtained for attack scenarios **S1**-**S4** in Fig. 3 highlight the superiority of LHESO and CESO in dealing with time-varying attack signals considered in **S2**-**S4**. Although NESO results in higher accuracy compared to LESO in **S2** and **S3** due to its nonlinear nature, the oscillation near steady state in **S1** and **S4** present a significant disadvantage in terms of practical implementation on real systems where measurement noise is always present.

VI. Conclusion

An ESO based actuator FDIA signal estimation approach was investigated in the present work. Through simulation study performed on a networked motion control platform, it was demonstrated that CESO and LHESO present a much better alternative to conventional linear and nonlinear ESO structures in terms of accuracy while estimating time varying FDIA signals as well as suppressing the effect of high-frequency measurement noise on the obtained estimates. In particular, it was shown that LHESO yields the best estimation performance while simultaneously addressing the numerical issue that restricts implementation of high-gain observers on fixed-point digital signal processors.

References

[1] Zhao, Y.B., Sun, X.M., Zhang, J. and Shi, P., 2015. Networked control systems: The communication basics and control methodologies. Mathematical Problems in Engineering.

[2] Ahmed, H, Ushirobira, R., and Efimov, D., Robust Global Synchronization of Brockett Oscillators, IEEE Transactions on Control of Network Systems, vol. 6, no. 1, pp. 289-298, Mar. 2019.

[3] Zhang, D., Wang, Q.G., Feng, G., Shi, Y. and Vasilakos, A.V., 2021. A survey on attack detection, estimation and control of industrial cyber-physical systems. ISA Transactions, 116, pp.1-16.

[4] Manson, S. and Anderson, D., 2019. Cybersecurity for protection and control systems: An overview of proven design solutions. IEEE Industry Applications Magazine, 25(4), pp.14-23.

[5] Falliere N, Murchu LO, Chien E. W32.stuxnet dossier. 2011, url- https://www.symantec.com/content/en/us/enterprise/media/securityresponse/whitepapers/w32-stuxnet-dossier.pdf.

[6] H. Sandberg, S. Amin, and K. H. Johansson, Cyberphysical security in networked control systems: An introduction to the issue, IEEE Control Systems Magazine, vol. 35, no. 1, pp. 20-23, Feb. 2015.

[7] How to Compromise PLC Systems via Stealthy Pin Control Attacks. url- https://securityaffairs.co/wordpress/53069/hacking/plcattacks.html.

[8] Cecilia, A., Sahoo, S., Dragicevic, T., Costa-Castello, R. and Blaabjerg, F., 2021. On Addressing the Security and Stability Issues Due to False Data Injection Attacks in DC Microgrids- An Adaptive Observer Approach. IEEE Transactions on Power Electronics.

[9] Chen, G., Zhang, Y., Gu, S. and Hu, W., 2021. Resilient State Estimation and Control of Cyber-Physical Systems Against False Data Injection Attacks on Both Actuator and Sensors. IEEE Transactions on Control of Network Systems.

[10] Manandhar, K., Cao, X., Hu, F. and Liu, Y., 2014. Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE Transactions on Control of Network Systems, 1(4), pp.370-379.

[11] Ju, Z., Zhang, H. and Tan, Y., 2020. Distributed deception attack detection in platoon-based connected vehicle systems. IEEE Transactions on Vehicular Technology, 69(5), pp.4609-4620.

[12] Hu, Y., Yang, A., Li, H., Sun, Y. and Sun, L., 2018. A survey of intrusion detection on industrial control systems. International Journal of Distributed Sensor Networks, 14(8), p.1550147718794615.

[13] Cecilia, A., Sahoo, S., Dragicevic, T., Costa-Castello, R. and Blaabjerg, F., 2021. Detection and Mitigation of False Data in Cooperative DC Microgrids With Unknown Constant Power Loads. IEEE Transactions on Power Electronics, 36(8), pp.9565-9577.

[14] Yang, T., Murguia, C., Kuijper, M. and Nesic, D., 2019, June. An unknown input multi-observer approach for estimation, attack isolation, and control of LTI systems under actuator attacks. In 2019 18th European Control Conference (ECC) (pp. 4350-4355). IEEE.

[15] Miao, K., Shi, X. and Zhang, W.A., 2020. Attack signal estimation for intrusion detection in industrial control system. Computers & Security, 96, p.101926.

[16] Ahmed, H., et al., A Fault Detection Method for Automatic Detection of Spawning in Oysters, IEEE Transactions on Control Systems Technology, vol. 24, no. 3, pp. 1140-1147, May. 2016.

[17] Ahmed, H., et al., 2015, July. Automatic spawning detection in oysters: a fault detection approach. In Proceedings of the European control conference (pp. 1140-1147).

[18] Lakomy, K. and Madonski, R., 2021. Cascade extended state observer for active disturbance rejection control applications under measurement noise. ISA transactions, 109, pp.1-10.

[19] Lakomy, K., Madonski, R., Dai, B., Yang, J., Kicki, P., Ansari, M. and Li, S., 2021. Active Disturbance Rejection Control Design with Suppression of Sensor Noise Effects in Application to DC-DC Buck Power Converter. IEEE Transactions on Industrial Electronics, early access.

[20] Ahmad, S. and Ali, A., 2021. On Active Disturbance Rejection Control in Presence of Measurement Noise. IEEE Transactions on Industrial Electronics, early access.

[21] Astolfi, D. and Marconi, L., 2015. A high-gain nonlinear observer with limited gain power. IEEE Transactions on Automatic Control, 60(11), pp.3059-3064.

[22] Astolfi, D., Marconi, L., Praly, L. and Teel, A.R., 2018. Low-power peaking-free high-gain observers. Automatica, 98, pp.169-179.

[23] Li, J., Xia, Y., Qi, X. and Gao, Z., 2016. On the necessity, scheme, and basis of the linear-nonlinear switching in active disturbance rejection control. IEEE Transactions on Industrial Electronics, 64(2), pp.1425-1435.

[24] Gao, Z., 2002. From linear to nonlinear control means: A practical progression. ISA transactions, 41(2), pp.177-189.

[25] Gao, Z., 2006, June. Scaling and bandwidth-parameterization based controller tuning. In Proceedings of the American control conference (Vol. 6, pp. 4989-4996).

[26] Khalil, H.K., 2017. High-gain observers in nonlinear feedback control. Society for Industrial and Applied Mathematics.

[27] Sira-Ramirez, H., 2018. From flatness, GPI observers, GPI control and flat filters to observer-based ADRC. Control Theory and Technology, 16(4), pp.249-260.