논문 2023-18-38

A Sliding Mode Observer for Reconstructing Cyber Attacks

Joseph Chang Lun Chan, Tae H. Lee*

Abstract : This paper presents a sliding mode observer (SMO) for reconstructing cyber attacks affecting a system. The system is first re-expressed such that its design freedom is easier to manipulate. The SMO is then used to reconstruct the cyber attack affecting the system. A simulation example is used to verify the performance of the SMO under two types of cyber attacks, and its results demonstrate the effectiveness of our proposed scheme.

Keywords : Cyber attack, Sliding mode observer, Estimator, Rank condition, Signal reconstruction

Ⅰ. Introduction

Modern industrial systems often consist of two separate layers: the cyber layer which consists of the information processing and communication network, and the physical layer which represents the subsystem interacting with the real world [1]. These systems are collectively referred to as cyber-physical systems (CPSs), and have been implemented across various fields, such as power systems, smart grids, transportation networks, and utility distribution networks [2, 3]. The separation between the two layers however is vulnerable to malicious external influences (hereafter referred to as cyber attacks), which could disrupt the regular operation of the system by corrupting or even falsifying transmitted data [4-6]. These disruptions could cause equipment damage and losses from downtime [7], and therefore it is important to be able to detect and reconstruct the cyber attacks if and when they occur.

Sliding mode observers (SMOs) are a popular method to reconstruct unknown inputs affecting a system [8]. The discontinuous switching term within SMOs can force estimation errors for the outputs to zero in finite time [9] (this is in contrast with other kinds of observers that can only achieve asymptotic convergence for state estimation [4]). Additionally, information regarding the unknown input can be derived from the switching term, which allows the unknown input to be reconstructed [10]. By treating the cyber attack as an unknown input, we can therefore determine if the system is under attack, and reconstruct it accordingly [11]. It is vital that the reconstruction accurately and quickly tracks the ongoing cyber attack [12], as it will be used in deploying the appropriate counter-measures in the CPS [13 - 15].

Motivated by these points, we propose a SMO for reconstructing cyber attacks affecting a system. The system will first be re-expressed to have structures that facilitate analysis, where the inherent design freedom is easily exploited. Next, the SMO to reconstruct the cyber attacks is designed. The Edwards-Spurgeon SMO structure is chosen for its ability to reconstruct the attack signal with minimal requirements and its compatibility with the system [16]. The efficacy of the proposed SMO is showcased using a simulation example of a practical system under two different cyber attacks.

The paper is organised as follows: Section 2 introduces the problem, and re-expresses the system into a form that is compatible with the observer. Section 3 then details the SMO used to reconstruct the cyber attacks, studies its performance, and presents a procedure to design the scheme. Next, Section 4 shows a simulation example to verify the performance of the SMO, and Section 5 concludes the paper. The following notation is used: the norm of a vector $a \in R^b$ is given by $\|a\| = \sqrt{\sum_{i=1}^{b} a_i^2}$, and the spectrum of a matrix E is labelled as $\lambda(E)$.

Ⅱ. Preliminaries

Consider the following system:

$$\dot{x_o}(t) = A_o x_o(t) + B_o(u(t) + f(t)), \quad (1)$$

$$y(t) = C_o x_o(t), \quad (2)$$

where $A_o \in R^{n \times n}$, $B_o \in R^{n \times m}$, and $C_o \in R^{p \times n}$ are known and constant matrices, $x_o(t)$, $u(t)$, $f(t)$, and $y(t)$ are the states, control inputs, cyber attacks, and outputs,

*Corresponding Author (thelee@jbnu.ac.kr)
Received: Sep. 13, 2023, Revised: Oct. 27, 2023, Accepted: Nov. 21, 2023.
J. C. L. Chan: Monash University, Malaysia
T. H. Lee: Jeonbuk National University (Assoc. Prof.)
※ 본 논문은 2023년도 정부 (과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. RS-2023-00210401).

ⓒ IEMEK J. Embed. Sys. Appl. 2023 Dec. 18(6) 311-317
ISSN : 1975-5066
http://dx.doi.org/10.14372/IEMEK.2023.18.6.311

respectively. Without loss of generality, B_o and C_o are assumed to be full-column rank and full-row rank, respectively, i.e., $rank(B_o)=m$, $rank(C_o)=p$.

The aim of the work is to reconstruct $f(t)$ using only $u(t)$ and $y(t)$. System (1)-(2) would first be transformed into a structure that facilitates later analysis. A sliding mode observer (SMO) is then utilized to reconstruct $f(t)$ based on $u(t)$ and $y(t)$.

The following assumptions are made to ease manipulation of the system structures:

Assumption 1 : $rank(C_0B_o)=m$.

Assumption 2 : $rank\begin{bmatrix}sI_n-A_o & B_o\\ C_o & 0\end{bmatrix}=n+m \quad \forall s\in C^+$.

Assumption 3 : The cyber-attack $f(t)$ is bounded, i.e., $\|f(t)\|\le \bar{f}$, where $\bar{f}$ is known.

Remark 1 : Assumptions 1-3 are standard for reconstructing unknown inputs using SMOs [16]. Assumption 1 implies that the cyber attacks only affect states that are measurable outputs, while Assumption 2 implies that system (1)-(2) is minimum phase. Assumption 3 is a practical assumption, as large cyber-attacks can easily be detected [17]. These assumptions will be required for the transformations in this section, as well as for the design of the SMO in the next section.

Define a matrix $N_C\in R^{n\times p}$ such that $C_oN_C=0$. Hence, define a non-singular matrix $T_a=\begin{bmatrix}N_C^T\\ C_o\end{bmatrix}$, which implies $C_oT_a^{-1}=[0, I_p]$. Apply the transformation $x_o(t)\mapsto T_ax_o(t)=x_a(t)$, and (1)-(2) can be re-expressed as

$$\dot{x}_a(t)=A_ax_a(t)+\underbrace{\begin{bmatrix}B_{a1}\\ B_{a2}\end{bmatrix}}_{B_a}(u(t)+f(t)), \tag{3}$$

$$y(t)=\underbrace{[0, I_p]}_{C_a}x_o(t), \tag{4}$$

where $A_a=T_aA_oT_a^{-1}$, $B_a=T_aB_o$, $B_{a1}\in R^{(n-p)\times m}$, $B_{a2}\in R^{p\times m}$, and $C_a=C_oT_a^{-1}$. We now use the following proposition to further re-express system (3)-(4) into a form that eases later analysis.

Proposition 1 : Suppose Assumption 1 is satisfied. Then there exist transformations allowing system (3)-(4) to be re-expressed as

$$\dot{x}_1(t)=(A_1+LA_3)x_1(t)+(A_2+LA_4-(A_1+LA_3)L)x_2(t), \tag{5}$$

$$\dot{x}_2(t)=A_3x_1(t)+(A_4-A_3L)x_2(t)+\bar{B}(u(t)+f(t)), \tag{6}$$

$$y(t)=C_2x_2(t), \tag{7}$$

where $L=[0, \bar{L}]\in R^{(n-p)\times p}$, $\bar{L}\in R^{(n-p)\times(p-m)}$, $\bar{B}=\begin{bmatrix}I_m\\ 0\end{bmatrix}\in R^{p\times m}$ while A_1, A_2, A_3, A_4, C_2, $x_1(t)\in R^{n-p}$, and $x_2(t)\in R^p$ are defined in the proof. Suppose also that Assumption 2 is satisfied. Then $\bar{L}$ can be chosen such that $\lambda(A_1+LA_3)<0$.

Proof : Assumption 1 implies $rank(B_{a2})=m$, which in turn implies there exist a matrix $T_{b1}\in R^{(n-p)\times p}$ and a non-singular matrix $T_{b2}\in R^{p\times p}$ satisfying $\begin{bmatrix}T_{b1}\\ T_{b2}\end{bmatrix}B_{a2}=\begin{bmatrix}-B_{a1}\\ \bar{B}\end{bmatrix}$. Therefore, define a non-singular matrix $T_b=\begin{bmatrix}I_{n-p} & T_{b1}\\ 0 & T_{b2}\end{bmatrix}$ and apply the transformation $x_a(t)\mapsto T_bx_a(t)=x_b(t)$ to re-express (A_a, B_a, C_a) as $C_aT_b^{-1}=[0, C_2]$ and

$$(A_a, B_a)\mapsto(T_bA_aT_b^{-1}, T_bB_a)=(A_b, B_b)=\left(\left[\begin{array}{cc|c}A_1 & A_2 & 0\\ A_3 & A_4 & \bar{B}\end{array}\right]\right), \tag{8}$$

where $A_1\in R^{(n-p)\times(n-p)}$, $A_2\in R^{(n-p)\times p}$, $A_3\in R^{p\times(n-p)}$, $A_4\in R^{p\times p}$, and $C_2=T_{b2}^{-1}$. Next, further partition A_3 as $A_3=\begin{bmatrix}A_{31}\\ A_{32}\end{bmatrix}$, where $A_{31}\in R^{m\times(n-p)}$ and $A_{32}\in R^{(p-m)\times(n-p)}$, define a non-singular matrix $T_c=\begin{bmatrix}I_{n-p} & L\\ 0 & I_p\end{bmatrix}$, and apply the transformation $x_b(t)\mapsto T_cx_b(t)=\begin{bmatrix}x_1(t)\\ x_2(t)\end{bmatrix}$ to transform the system to have the structures in (5)-(7).

Then since T_a, T_b, T_c, and C_2 are non-singular, the structures in (5)-(8) imply

$$\begin{aligned}
&rank\begin{bmatrix}sI_n-A_o & B_o\\ C_o & 0\end{bmatrix}\\
&=rank\begin{bmatrix}T_cT_bT_a & 0\\ 0 & I_p\end{bmatrix}\begin{bmatrix}sI_n-A_o & B_o\\ C_o & 0\end{bmatrix}\begin{bmatrix}(T_cT_bT_a)^{-1} & 0\\ 0 & I_m\end{bmatrix}\\
&=rank\begin{bmatrix}sI_{n-p}-(A_1+LA_3) & -(A_2+LA_4-(A_1+LA_3)L) & 0\\ -A_3 & sI_p-(A_4-A_3L) & \bar{B}\\ 0 & C_2 & 0\end{bmatrix}\\
&=rank\begin{bmatrix}I_{n-p}-L\\ 0 \quad I_p\end{bmatrix}\begin{bmatrix}sI_{n-p}-A_1\\ A_{32}\end{bmatrix}+p+m\\
&=\underbrace{rank\begin{bmatrix}sI_{n-p}-A_1\\ A_{32}\end{bmatrix}}_{E(s)}+p+m.
\end{aligned} \tag{9}$$

Assumption 2 implies $rank(E(s))=n-p \quad \forall s\in C^+$, and by using the Popov-Hautus-Rosenbrock (PHR) rank test [11], the unobservable modes of (A_1, A_{32}) (i.e., the values of s that cause $E(s)$ to lose rank) are stable, i.e., (A_1, A_{32}) is

detectable. Hence $\bar{L}$ can always be chosen such that $\lambda(A_1+\bar{L}A_{32})=\lambda(A_1+LA_3)<0$. Thus, the proof is complete. ■

System (1) - (2) has been re-expressed in the form of (5) - (7), which is compatible with the Edwards-Spurgeon SMO [16].

Ⅲ. The Observer for Cyber Attack Reconstruction

In this section, we present the SMO to reconstruct $f(t)$ and analyse its performance. Afterwards, we give a summarized design procedure. The Edwards-Spurgeon SMO [16] for system (5) - (7) is given by

$$\dot{\hat{x}}_1(t)=(A_1+LA_3)\hat{x}_1(t)+(A_2+LA_4-(A_1+LA_3)L)C_2^{-1}y(t), \quad (10)$$

$$\dot{\hat{x}}_2(t)=A_3\hat{x}_1(t)+(A_4-A_3L)\hat{x}_2(t)+\bar{u}(t)+v(t) +(C_2^{-1}\bar{A}-(A_4-A_3L)C_2^{-1})(\hat{y}(t)-y(t)), \quad (11)$$

$$\hat{y}(t)=C_2\hat{x}_2(t), \quad (12)$$

$$v(t)=-\rho C_2^{-1}\frac{\hat{y}(t)-y(t)}{\|\hat{y}(t)-y(t)\|}, \quad (13)$$

where $v(t)\in R^{p\times p}$ is the sliding term, and $\bar{A}\in R^{p\times p}$ and $\rho\in R^{+}$ are design parameters which will be designed in the following subsection.

1. Observer performance analysis

Define the errors $e_1(t)=\hat{x}_1(t)-x_1(t)$ and $e_y(t)=\hat{y}(t)-y(t)$. By using (5)-(7) and (10)-(13), the following error system (which characterises the performance of the SMO) can be derived:

$$\dot{e}_1(t)=(A_1+\bar{L}A_{32})e_1(t), \quad (14)$$

$$\dot{e}_y(t)=C_2A_3e_1(t)+\bar{A}e_y(t)-C_2\bar{B}f(t)+C_2v(t). \quad (15)$$

We now show how sliding motion is achieved in SMO (9)-(13) using the following proposition:

Proposition 2 : Suppose that for a given positive scalar α, there exist a symmetric positive-definite matrix $P\in R^{(n-p)\times(n-p)}$ and any matrix $K\in R^{(n-p)\times(n-p)}$ satisfying the inequality

$$PA_1+KA_{32}+(PA_1+KA_{32})^T+\alpha P<0. \quad (16)$$

Suppose also that SMO (9)-(13) is designed using $\bar{L}=P^{-1}K$ and

$$\bar{A}<0, \quad (17)$$

$$\rho>\|C_2A_3\|\beta+\|C_2\bar{B}\|\bar{f}, \quad (18)$$

where $\beta>\|e_1(0)\|\sqrt{\frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}}$. Then an ideal sliding motion for error system (14)-(15) on the surface $S=\{e_1(t),e_y(t):e_y(t)=0\}$ can be achieved in finite time.

Proof : We split the proof into two portions: the first part shows how $e_1(t)$ is bounded by β, while the second part would show how sliding motion on S is achieved in finite time.

First define the Lyapunov candidate function $V_1(t)=e_1^T(t)Pe_1(t)$, and differentiating it with respect to time gives

$$\dot{V}_1(t)=e_1^T(t)\left(P(A_{1+}\bar{L}A_{32})+(A_1+\bar{L}A_{32})^TP\right)e_1(t). \quad (19)$$

Next, substitute for P and K into inequality (16) to obtain

$$P(A_1+\bar{L}A_{32})+(A_1+\bar{L}A_{32})^TP+\alpha P<0. \quad (20)$$

Satisfying (16) therefore implies $\dot{V}_1(t)<-\alpha e_1^T(t)Pe_1(t)=-\alpha V_1(t)$, which in turn implies that $\|e_1(t)\|\le\|e_1(0)\|\exp\{-\alpha/2\}\sqrt{\frac{\lambda_{\max}(P)}{\lambda_{\min}(P)}}\le\beta$ [18]. This completes the first portion of the proof.

In the next and final part of the proof, we show how setting $\bar{A}$ and ρ according to (17)-(18) would yield sliding motion on S in finite time. Define a second Lyapunov candidate function $V_y(t)=e_y^T(t)e_y(t)$, and differentiating it with respect to time gives

$$\dot{V}_y(t)=2e_y^T(t)(C_2A_3e_1(t)-C_2\bar{B}f(t)+C_2v(t)) +e_y^T(t)(\bar{A}+\bar{A}^T)e_y(t). \quad (21)$$

Substituting for $v(t)$ from (13) and setting $\bar{A}$ according to (17) result in

$$\dot{V}_y(t)<-2\|e_y(t)\|(\rho-\|C_2A_3\|\beta-\|C_2\bar{B}\|\bar{f}). \quad (22)$$

Then by setting ρ according to (18), we obtain $\dot{V}_y(t)<-2\gamma\|e_y(t)\|<-2\gamma\sqrt{V_y(t)}$, where γ is an arbitrary positive constant. This is the reachability condition [19], which results in $e_y(t)=0$ in finite time. Therefore, a sliding motion is induced on S in finite time, and the proof is complete. ■

We now show how $f(t)$ is reconstructed by SMO (9)-(13) using the following theorem:

Theorem 1 : SMO (9)-(13) can reconstruct $f(t)$ if and only if Propositions 1 and 2 are satisfied.

Proof : Satisfying Proposition 1 would allow system (1)-(2) to be re-expressed as (5)-(7), which is compatible with SMO (9)-(13). The satisfaction of Proposition 2 results in sliding motion on S taking place in finite time, after which $e_y(t)=0$, $\dot{e}_y(t)=0$ and error system (14)-(15) becomes

$$\dot{e}_1(t)=(A_1+\bar{L}A_{32})e_1(t), \tag{23}$$
$$0=C_2(A_3e_1(t)-\bar{B}f(t)+v_{eq}(t)), \tag{24}$$

where $v_{eq}(t)$ is the equivalent output error injection required to maintain sliding motion on S. Rearrange (24), and by substituting for the structures of A_3 and $\bar{B}$ from Proposition 1, we get

$$v_{eq}(t)=\begin{bmatrix}-A_{31}\\-A_{32}\end{bmatrix}e_1(t)+\begin{bmatrix}I_m\\0\end{bmatrix}f(t). \tag{25}$$

Hence define the attack reconstruction $\hat{f}(t)$ and the attack reconstruction error $e_f(t)$ as

$$\hat{f}(t)=[I_m,0]v_{eq}(t),\quad e_f(t)=\hat{f}(t)-f(t), \tag{26}$$

respectively. Using (25)-(26), we obtain $e_f(t)=-A_{31}e_1(t)$. Recall from Proposition 2 that as $t\to\infty$, $e_1(t)\to 0$ which would in turn imply that as $t\to\infty$, $e_f(t)\to 0$. Thus $\hat{f}(t)\to f(t)$, completing the proof. ■

2. Design algorithm

A summarised design procedure for the SMO for cyber attack reconstruction is given in the following:

Step 1. Check if Assumptions 1-3 hold. If not, stop as the scheme is not applicable.

Step 2. Calculate T_a from before (3) and T_b from Proposition 1.

Step 3. Apply the transformation $x_o(t)\mapsto T_bT_ax_o(t)$ to obtain the structures in (8).

Step 4. Select a value for α in Proposition 2, and apply a linear matrix inequality (LMI) solver on inequality (16) to obtain P and K.

Step 5. Calculate $\bar{L}=P^{-1}K$, and choose $\bar{A}$ and ρ to satisfy (17)-(18), respectively.

Step 6. Reconstruct $f(t)$ using (26).

Ⅳ. Simulation Example

To demonstrate the performance of our scheme, consider a modified version of the mechanical system with two masses and springs in [20]. Suppose that the input into the system is susceptible to cyber attacks, and we want to reconstruct the cyber attack $f(t)$ when it occurs. The matrices (A_o,B_o) in (1) are given by

$$A_o=\begin{bmatrix}0&0&1&0\\0&0&0&1\\-2&1&-0.5&0\\2&-2&0&-1\end{bmatrix},\ B_o=\begin{bmatrix}0\\0\\1\\0\end{bmatrix}, \tag{27}$$

for system variables

$$x_o(t)=\begin{bmatrix}p_1(t)\\p_2(t)\\v_1(t)\\v_2(t)\end{bmatrix},\ u(t)=F(t), \tag{28}$$

where $p_1(t)$, $p_2(t)$, $v_1(t)$, $v_2(t)$, $F(t)$ denoting the position of mass 1 and 2, velocity of mass 1 and 2, and driving force, respectively.

Suppose only $p_1(t)$, $p_2(t)$, and $v_1(t)$ are measured. Thus, C_o in (2) has the form

$$C_o=[I_3,0]. \tag{29}$$

We now design the scheme to reconstruct $f(t)$ according to the procedure outlined in subsection 3.2.

Step 1. From (27)-(29), we obtain

$$rank(C_oB_o)=1,\ m=1,\ rank\begin{bmatrix}sI_4-A_o,B_o\\C_o,\quad 0\end{bmatrix}=5,\ \forall s\in C^+. \tag{30}$$

This implies Assumptions 1 and 2 are satisfied. Furthermore, we assume that $f(t)$ is bounded by $\bar{f}=1.5$, and hence Assumption 3 is also satisfied.

Step 2. The matrices T_a and T_b were calculated to be

$$T_a=\begin{bmatrix}0&1\\I_3&0\end{bmatrix},\ T_b=\begin{bmatrix}1&0&0\\0&0&1\\0&I_2&0\end{bmatrix}. \tag{31}$$

Step 3. System (27)-(29) is then re-expressed as

$$A_b=\begin{bmatrix}-1&0&2&-2\\0&-0.5&-2&1\\0&1&0&0\\1&0&0&0\end{bmatrix},\ B_b=\begin{bmatrix}0\\1\\0\\0\end{bmatrix},\ C_b=\begin{bmatrix}0&0&I_n\\0&1&0\end{bmatrix}. \tag{32}$$

Step 4. The LMI parameter α is set as $\alpha=1$. Using the SeDuMi solver for YALMIP in MATLAB, we obtain

$$P=7.377,\ K=[4.266,2.688]. \tag{33}$$

Step 5. The observer parameters are set as $\bar{A}=-10$ and $\rho=10$, while $\bar{L}$ is calculated to be $\bar{L}=[0.5783,0.3644]$.

Step 6. The cyber attack is therefore reconstructed using

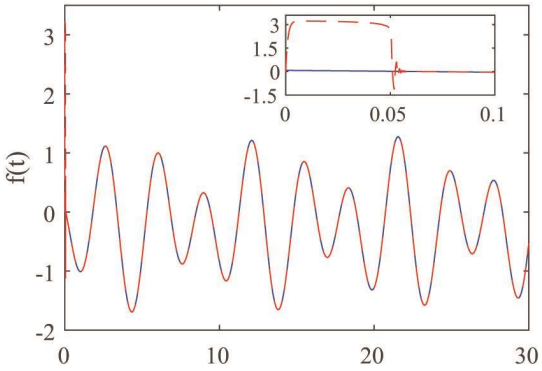

Fig. 1. The reconstruction of the attack in the first scenario

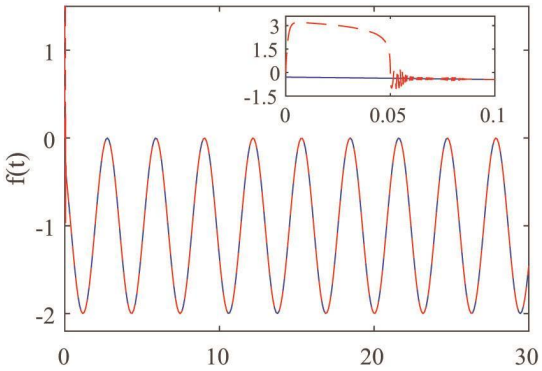

Fig. 2. The reconstruction of the attack in the second scenario.

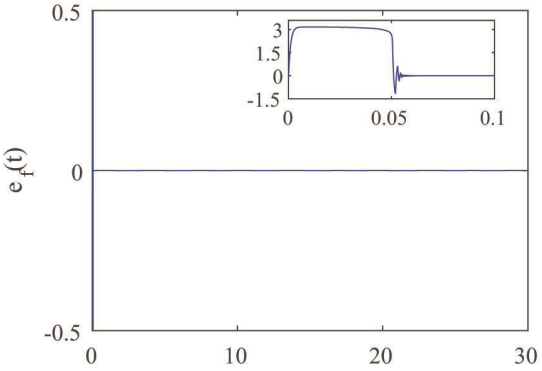

Fig. 3. The attack reconstruction error in the first scenario.

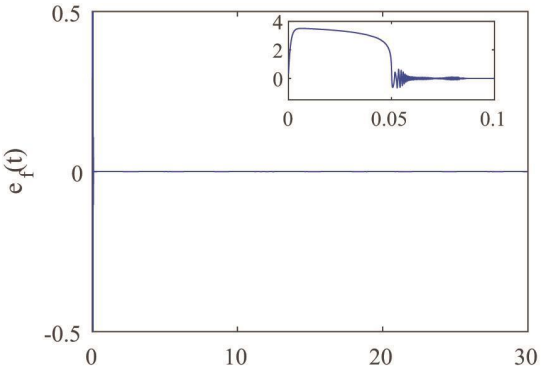

Fig. 4. The attack reconstruction error in the second scenario.

$$\hat{f}(t) = [1, 0, 0, 0]v_{eq}(t). \tag{34}$$

The design of the observer proposed in this paper is now complete. To show the effectiveness of the scheme in reconstructing the attack, we simulate two scenarios: the first scenario involves a Denial-of-Service (DoS) attack which zeros the effect of $u(t)$ entirely, i.e., $f(t) = -u(t)$ [21]. The second scenario considers a deception attack, where the attacker removes the influence of $u(t)$ and injects the attack signal $a(t)$, i.e., $f(t) = -u(t) + a(t)$ [22]. In both cases, system (27)-(29) has the initial condition $\{0.5, 0.3, 0.2, 0.4\}$, while the observer is set to have zero initial conditions. The input $u(t)$ and the attack signal in the second scenario are respectively set as

$$u(t) = 1 + \sin(2t + 7\pi/4),\ a(t) = 0.8 + 0.5\sin(1.3t + 5\pi/3). \tag{35}$$

Figs. 1 and 2 show the reconstructions of the attacks in the first and second scenarios, respectively. It can be seen that after some transient dynamics at the start arising from the differing initial conditions, the attacks are faithfully reconstructed. The faithfulness of the reconstruction can be demonstrated using the attack reconstruction error, which we define as

$$e_f(t) = \hat{f}(t) - f(t). \tag{36}$$

Figs. 3 and 4 show the attack reconstruction errors in the first and second scenarios, respectively. There are also initial transients present in the attack reconstruction errors, but these quickly vanish and the errors go to zero and remain there afterwards. Thus, the proposed observer scheme has been shown to be effective for reconstructing cyber attacks.

V. Conclusion

This paper has presented a SMO to reconstruct cyber attacks using only the inputs and outputs of a system. The system was first re-expressed into a form that facilitates further analysis. The SMO for cyber attack reconstruction was then designed for the system. A simulation example was carried out, where two different forms of cyber attacks were considered. The results of the simulation demonstrate the efficacy of the proposed scheme.

References

[1] H. S. Sánchez, D. Rotondo, T. Escobet, V. Puig, J. Quevedo, "Bibliographical Review on Cyber Attacks from a Control Oriented Perspective," Annu. Rev. Control, Vol. 48, pp. 103-128, 2019.

[2] D. Ye, S. Luo, "A Co-design Methodology for Cyber-physical Systems Under Actuator Fault and Cyber Attack," J. Franklin Inst., Vol. 356, No. 4, pp. 1856-1879, 2019.

[3] L. Shi, Q. Dai, Y. Ni, "Cyber-physical Interactions in Power Systems: a Review of Models, Methods, and Applications," Electr. Power Syst. Res., Vol. 163, Part A, pp. 396-412, 2018.

[4] P. Wen, N. Hou, Y. Shen, J. Li, Y. Zhang, "Observer-based H∞ PID Control for Discrete-time Systems Under Hybrid Cyber Attacks," Syst. Sci. Control Eng., Vol. 9, No. 1, pp. 232-242, 2021.

[5] T. H. Lee, "Control of Cyber-Physical Systems Under Cyber-Attacks," IEMEK J. Embed. Sys. Appl., Vol. 14, No. 5, pp. 269-275, 2019. (in Korean)

[6] J. H. Kim, D. G. Kim, D. I. Lee, "Kalman Filter Based Resilient Cyber-Physical System and its Application to an Autonomous Vehicle," IEMEK J. Embed. Sys. Appl., Vol. 14, No. 5, pp. 239-247, 2019. (in Korean)

[7] A. Barboni, H. Rezaee, F. Boem, T. Parisini, "Detection of Covert Cyber-attacks in Interconnected Systems: a Distributed Model-based Approach," IEEE Trans. Automat. Control, Vol. 65, No. 9, pp. 3728-3741, 2020.

[8] H. Yang, Y. Jiang, S. Yin, "Fault-tolerant Control of Time-delay Markov Jump Systems with Itô Stochastic Process and Output Disturbance Based on Sliding Mode Observer," IEEE Trans. Ind. Inform., Vol. 14, No. 12, pp. 5299-5307, 2018.

[9] L. Zhang, G. Guo, "Observer-based Adaptive Event-triggered Sliding mode Control of Saturated Nonlinear Networked Systems with Cyber-attacks," Inf. Sci., Vol. 543, pp. 180-201, 2021.

[10] L. Ye, F. Zhu, J. Zhang, "Sensor Attack Detection and Isolation Based on Sliding mode Observer for Cyberphysical Systems," Int. J. Adapt. Control Signal Process., Vol. 34, No. 4, pp. 469-483, 2020.

[11] J. C. L. Chan, T. H. Lee, "Sliding mode Observer-based Fault-tolerant Secondary Control of Microgrids," Electron., Vol. 9, pp. 1-23, 2020.

[12] L. Li, W. Wang, Q. Ma, K. Pan, X. Liu, L. Lin, J. Li, "Cyber Attack Estimation and Detection for Cyberphysical Power Systems," Appl. Math. Comput., Vol. 400, Article No. 126056, 2021.

[13] A. Di Giorgio, A. Pietrabissa, F. Delli Priscoli, A. Isidori, "Robust Protection Scheme Against Cyberphysical Attacks in Power Systems," IET Control Theory Appl., Vol. 12, No. 13, pp. 1792-1801, 2018.

[14] P. S. P. Pessim, M. J. Lacerda, "State-feedback Control for Cyber-physical LPV Systems Under DoS Attacks," IEEE Control Syst. Lett., Vol. 5, No. 3, pp. 1043-1048, 2021.

[15] T. Yucelen, W.M. Haddad, E. M. Feron, "Adaptive Control Architectures for Mitigating Sensor Attacks in Cyber-physical Systems," Cyber-Phys. Syst., Vol. 2, No. 1 - 4, pp. 24-52, 2016.

[16] H. Alwi, C. Edwards, C. P. Tan, "Fault Detection and fault-Tolerant Control Using Sliding Modes (Advances in Industrial Control)," London, U.K.: Springer, 2011.

[17] D. Zhao, Z. Wang, G. Wei, Q. L. Han, "A Dynamic Event-triggered Approach to Observer-based PID Security Control Subject to Deception Attacks," Automatica, Vol. 120, Article No. 109128, 2020.

[18] X. G. Yan, C. Edwards, "Nonlinear Robust Fault Reconstruction and Estimation Using a Sliding mode Observer," Automatica, Vol. 43, No. 9, pp. 1605-1614, 2007.

[19] C. P. Tan, C. Edwards, "Sliding mode Observers for Robust Detection and Reconstruction of Actuator and Sensor Faults," Int. J. Robust Nonlinear Control, Vol. 13, No. 5, pp. 443-463, 2003.

[20] T. H. Lee, C. P. Lim, S. Nahavandi, R. G. Roberts, "Observer-based H∞ Fault-tolerant Control for Linear Systems with Sensor and Actuator Faults," IEEE Syst. J., Vol. 13, No. 2, pp. 1981-1990, 2019.

[21] F. Li, X. Yan, Y. Xie, Z. Sang, X. Yuan, "A Review of Cyber-attack Methods in Cyber-physical Power System," in Proc. IEEE 8th Int. Conf. Adv. Power Syst. Autom. Prot. (APAP), 2019, pp. 1335-1339.

[22] R. Meira-Góes, E. Kang, R. H. Kwong, S. Lafortune, "Synthesis of Sensor Deception Attacks at the Supervisory Layer of Cyber-physical Systems," Automatica, Vol. 121, No. 109172, 2020.

Joseph Chang Lun Chan

2013 School of Engineering, Monash University, Malaysia (B. Eng.)

2019 School of Engineering, Monash University, Malaysia (Ph.D.)

2019~2021 Electronic Engineering, Jeonbuk National University (Researcher)

2021~School of Engineering, Monash University, Malaysia (Researcher)

Field of Interests: Sliding Mode Observer, Fault Reconstruction

Email: joseph.chan1@monash.edu,

Tae H. Lee

2011 Electrical Engineering from Yeungnam University (M.S.)
2015 Electrical Engineering from Yeungnam University (Ph.D.)
2015~2016 Electrical Engineering in Yeungnam University (Researcher)
2017~2020 Electronic Engineering in Jeonbuk National University (Assistant Prof.)
2020~Electronic Engineering in Jeonbuk National University (Associate Prof.)
Career:
2017~ Editorial Committee, IeMeK
Field of Interests: Control Theory
Email: thlee@jbnu.ac.kr