Hindawi
Mathematical Problems in Engineering
Volume 2019, Article ID 7280474, 13 pages
https://doi.org/10.1155/2019/7280474

Research Article

A Multiplicative Coordinated Stealthy Attack for Nonlinear Cyber-Physical Systems with Homogeneous Property

Gyujin Na,[1] **Hanbit Lee**,[2] **and Yongsoon Eun**[1]

[1]*Department of Information and Communication Engineering, DGIST, Daegu, Republic of Korea*
[2]*Department of Research and Development, Agency for Defense Development (ADD), Daejeon, Republic of Korea*

Correspondence should be addressed to Yongsoon Eun; yeun@dgist.ac.kr

Received 28 February 2019; Accepted 18 July 2019; Published 29 August 2019

Academic Editor: Boulaïd Boulkroune

Copyright © 2019 Gyujin Na et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Stealthy attacks to cyber-physical systems (CPS) refer to the ones that avoid attack detection mechanisms augmented to the systems typically in the form of anomaly detectors. Various types of stealthy attacks have been reported in the literature. Among the attacks with stealthy property, a recently reported multiplicative coordinated attack is particularly dangerous in that it corrupts sensor and actuator data in a coordinated manner, and it does not require precise system knowledge in order to be stealthy. It must be noted that most of these attacks are applicable to CPS, the physical counterparts of which are of linear dynamics. This could be a limitation since most of the physical dynamic systems that are encountered from CPS perspective are of nonlinear nature. In this work, we present a version of multiplicative coordinated stealthy attack for a class of CPS, the physical counterpart of which possesses nonlinear dynamics. Specifically, for the physical systems with homogeneous property, the attack is constructed and the effect is analyzed. Various simulations are carried out to illustrate the effect of the attack.

1. Introduction

The improvement of computing power in embedded systems and significant advances of communication and network technologies have created a new field of cyber-physical systems (CPS) which tightly integrate physical and cyber components. Over the past years, CPS has emerged as an important paradigm to design large-scale distributed systems such as electric power grid systems, water distribution systems, and smart vehicular systems [1, 2]. However, recently, the cases where anonymous attackers penetrate the network systems and compromise CPS have increased [3]. The cyber attacks on CPS have caused considerable damages of the physical processes and brought enormous losses in property. The representative attack cases include the attack on Maroochy Shire Council's sewage control systems [4] and the Stuxnet worm virus attack on Supervisory Control and Data Acquisition (SCADA) systems [5].

For developing countermeasures for the known attacks [6–9, 10], comprehensive analysis of the feasible cyber attack mechanisms should be preceded. To date, many cyber attack mechanisms have been discovered and analyzed in [11–19]. The representative attack methodologies include Denial of Service (DoS) attack [11], replay attack [12, 13], bias injection attack [14], zero dynamics attack [15], robust zero dynamics attack [16], robust pole dynamics attack [17], data-driven covert attack [18], etc. The DoS attack is a jamming method for obstructing data transmission, which is realized by injecting a considerable amount of requests into specific communication channels. The replay attack is an attack method realized by recording sensor measurement outputs for an extended period of time and replacing the measurements with the stored data. The bias injection attack is a type of false data injection attack, which is achieved by injecting the arbitrary constant in the control or sensor signals. The zero dynamics attack is a model based on stealthy attack method, and the attackers generate the sophisticated attack signals using unstable zero dynamics of the targeted system. While the zero dynamics attack requires the exact model knowledge of the target system, the robust zero dynamics attack was developed based on a robust control tool called as a disturbance observer. The attack

corrupts the plant without the needs of the exact model knowledge and maintains the stealthiness for finite period. Robust pole dynamics attack is similar but applicable to linear systems with unstable dynamics. The data-driven covert attack is the attack strategy which can compromise the linear systems with parameter uncertainties. The attack utilizes a least mean square method for the parameter estimation, and the attack signals calculated from the estimated model are simultaneously injected into the input and output channels.

Fortunately, the existing attack methods reported in [11–18] have restrictions. For achieving the DoS attack, the attackers need much resources in that all possible communication channels should be occupied. The replay attack can be easily detected by watermarking the actuator signals. This is because the recorded output signals do not respond to the watermarks coded in the signals. The bias injection attack is not perfectly stealthy, which can be easily detected by anomaly detectors designed for monitoring the anomalous operations. The zero dynamics and robust zero dynamics attacks are dangerous only for the systems with nonminimum phase zeros. Robust pole dynamics attack is only to systems with unstable poles. The data-driven covert attack needs the minimum model knowledge such as the system dimension, although the complete model knowledge is not known to the attackers.

Recently, a notable stealthy attack mechanism capable of overcoming the said restrictions was developed in [19]. The attack is named a multiplicative coordinated stealthy attack and follows the method which multiplicatively compromises both the sensor and control signals in a coordinated manner. The attack design does not require model knowledge as long as the target system is linear. It is not detected by the watermarking technique. The applicability of the attack is not limited to the systems with nonminimum phase zeros nor unstable dynamics. The current work of the multiplicative coordinated stealthy attack introduced in [19], however, has focused on compromising the CPS, the physical counterpart of which is of linear dynamics. In this paper, as an extension of the attack to a class of CPS whose physical counterpart is of nonlinear dynamics, we specifically show that the multiplicative coordinated stealthy attack can compromise target CPS whose physical counterpart is of linear dynamics or of nonlinear dynamics with homogeneous property [20–22].

Main research interest of this paper is to reveal that a multiplicative coordinated stealthy attack is applicable to CPS with nonlinear physical plants with homogeneous property and to carry out relevant analysis. We show that the multiplicative coordinated attack is capable of forcing the states of target system far away from the desired trajectories without being detected. Attackers only need to know homogeneity degrees of the target systems. The attack can be realized, even if the attackers have incorrect information about the physical plant and have insufficient knowledge of the controller and the anomaly detector. The comparison with existing attacks (e.g., replay attack and false data injection attack) emphasizes that the multiplicative coordinated attack is particularly dangerous. Finally, two methods capable for detecting the multiplicative coordinated stealthy attacks are briefly discussed and demonstrated through simulations.

It should be noted that the security problem of the nonlinear dynamical systems has been rarely discussed in [23–25], while most of the systems have the nonlinearity. The problem of the attack detection and isolation for a class of discrete time nonlinear systems under sensor attack was addressed in [23]. The paper of Kim et al. [24] presented a detection method for the sensor attack and developed a resilient state estimation algorithm for uniformly observable nonlinear systems. The authors in [25] considered the sampled data consensus problem for a class of nonlinear multiagent systems under cyber attack.

The rest of this paper is organized as follows. In Section 2, mathematical preliminaries in order to define homogeneous systems are presented. In Section 3, we introduce a class of the nonlinear CPS and the multiplicative coordinated stealthy attack method for homogeneous nonlinear systems is proposed and analyzed. Various simulations are conducted in Section 4. The detection methods for the attack are briefly discussed in Section 5. Finally, conclusions are formulated in Section 6. All proofs are included in Appendix.

2. Mathematical Preliminaries

Before presenting a stealthy attack method for nonlinear homogeneous systems, we here introduce the basic definitions of homogeneity and the properties. The notion of homogeneity was first introduced in [26] for the stability analysis of a nonlinear system, which has led to interesting results as reported in [20–22]. In order to understand whether any function or system has the homogeneous property or not, the concept of dilation is required, and we simply introduce the definition below.

Definition 1. For fixed coordinates $x = (x_1, x_2, \ldots, x_n)^T \in \mathbb{R}^n/\{0\}$ and real numbers $r_i > 0$ for $1 \le i \le n$, a dilation $\Delta_\varepsilon^r : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is defined as

$$\Delta_\varepsilon^r x = \left(\varepsilon^{r_1} x_1, \varepsilon^{r_2} x_2, \ldots, \varepsilon^{r_n} x_n\right)^T, \tag{1}$$

where $\varepsilon > 0$ with r_i being called as homogeneous weights of x [20–22].

Now, by using the dilation, we can define the homogeneous function. Definition 2 shows the definition of the homogeneous function, and Lemma 1 shows that the homogeneous functions have a property.

Definition 2. A function $U : \mathbb{R}^n \longrightarrow \mathbb{R}$ is said to be a generalized homogeneous function of degree $k \in \mathbb{R}$ with respect to a dilation Δ_ε^r with an exponent r, if the following equality holds

$$U\left(\Delta_\varepsilon^r x\right) = \varepsilon^k U(x), \tag{2}$$

for all $\varepsilon > 0$. If the exponent r is $(1, \ldots, 1)$, the function $U(x)$ is said to be a classical homogeneous function [20–22].

Lemma 1. *Let $\rho > 0$ be an arbitrary constant. Consider a homogeneous function $U(x)$ of degree τ with respect to Δ_ε^r. ien, $U(x)$ is homogeneous of degree $\rho\tau$ with respect to $\Delta_\varepsilon^{\rho r}$* [20–22].

In next section, we first introduce a CPS and focus on the attack scenario where physical plants are remotely controlled via some unreliable communication network, and the attackers can penetrate such network systems without any restriction. Next, we show that a coordinated attack method can be applied into the nonlinear physical plants with homogeneous properties.

3. A Multiplicative Coordinated Stealthy Attack in Cyber-Physical Systems

3.1. A Cyber-Physical System. In this subsection, we briefly discuss a common CPS including a physical plant, a controller, and an anomaly detector. First consider a class of the controllable canonical nonlinear plants on the physical layer which is given by

$$\begin{aligned} \dot{x} &= Ax + B\left(f_n(x) + g_n(x)\widetilde{u}\right), \\ y &= h_n(x), \quad \forall x \in \Omega_x, \end{aligned} \tag{3}$$

where $x = (x_1, x_2, \ldots, x_n)^T \in \mathbb{R}^n$ is the plant state, $\widetilde{u} \in \mathbb{R}$ is the control input containing actuator attack signal, $y \in \mathbb{R}$ is the system output, $f_n : \mathbb{R}^n \longrightarrow \mathbb{R}$, $g_n : \mathbb{R}^n \longrightarrow \mathbb{R}$, and $h_n : \mathbb{R}^n \longrightarrow \mathbb{R}$ are continuous and smooth mapping, and Ω_x denotes the compact set of x. The matrices A and B are, respectively, defined as

$$\begin{aligned} A &= \begin{bmatrix} 0_{n-1} & I_{n-1} \\ 0 & 0_{n-1}^{\mathrm{T}} \end{bmatrix} \in \mathbb{R}^{n\times n}, \\ B &= \begin{bmatrix} 0_{n-1} \\ 1 \end{bmatrix} \in \mathbb{R}^n, \end{aligned} \tag{4}$$

where $I_{n-1} \in \mathbb{R}^{(n-1)\times(n-1)}$ is the identity matrix and $0_{n-1} \in \mathbb{R}^{n-1}$ is the zero vector.

Next, we consider a controller given by

$$\begin{aligned} \dot{c} &= \mathscr{C}(c, \widetilde{y}, y_r), \\ u &= \mathscr{U}(c, \widetilde{y}, y_r), \end{aligned} \tag{5}$$

where $c \in \mathbb{R}^m$ is the controller state, $\widetilde{y} \in \mathbb{R}$ is the sensor output including sensor attack, $y_r \in \mathbb{R}$ is the desired reference assumed to be sufficiently smooth and bounded, $u \in \mathbb{R}$ is the bounded controller output, and $\mathscr{C}(\cdot)$ and $\mathscr{U}(\cdot)$ are continuous and smooth mappings. Without loss of generality, it is assumed that the controller (5) is designed such that the system output follows some desired reference trajectory under attack-free condition and it is capable of forcing x to follow the desired reference y_r in Ω_x.

Before introducing the anomaly detector, we assume that (3) satisfies following Assumption 1. This is necessary for constructing the uniformly nonlinear observer in the anomaly detector [27] and guarantees the observability for all control inputs u.

Assumption 1. There exists a diffeomorphism function $\Xi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ such that (3) is transformed into

$$\begin{aligned} \dot{s} &= \begin{bmatrix} \dot{s}_1 \\ \dot{s}_2 \\ \vdots \\ \dot{s}_n \end{bmatrix} = \begin{bmatrix} s_2 \\ s_3 \\ \vdots \\ \alpha_n(s) \end{bmatrix} + \begin{bmatrix} \beta_1(s_1) \\ \beta_2(s_1, s_2) \\ \vdots \\ \beta_n(s) \end{bmatrix} \widetilde{u}, \\ y &= Cs = s_1, \end{aligned} \tag{6}$$

where $\alpha_n(\cdot)$ and $\beta_j(\cdot)$ for $1 \le j \le n$ are globally Lipschitz in s, and $C \coloneqq (1, 0, \ldots, 0) \in \mathbb{R}^n$.

For monitoring the system behavior of (3) and detecting the anomalous operations, the anomaly detector is commonly designed. The anomaly detector can be combined with (5) and consists of a full state observer [24, 28], a residue signal monitoring system, and an alarm system, which is represented by

$$\begin{aligned} \dot{z} &= \begin{bmatrix} z_2 \\ z_3 \\ \vdots \\ \alpha_n(z) \end{bmatrix} + \begin{bmatrix} \beta_1(z_1) \\ \beta_2(z_1, z_2) \\ \vdots \\ \beta_n(z) \end{bmatrix} u - P^{-1}C^T\gamma, \\ \widehat{y} &= Cz, \\ \gamma &= \widehat{y} - \widetilde{y}, \\ \gamma_d &= \|\gamma\|, \end{aligned} \tag{7}$$

where $z = (z_1, z_2, \ldots, z_n)^T \in \mathbb{R}^n$ is the estimated state for (6), $\widehat{y} \in \mathbb{R}$ is the observer output, $\gamma \in \mathbb{R}$ is the residue signal, and $P \in \mathbb{R}^{n\times n}$ is the positive definite solution of

$$0_{n\times n} = -\theta P - PA - A^T P + C^T C, \tag{8}$$

with the observer design parameter $\theta > 1$ and $0_{n\times n} \in \mathbb{R}^{n\times n}$. The anomaly detector in (7) will trigger the alarm if and only if

$$\|\gamma\| > \delta_T, \tag{9}$$

where $\delta_T > 0$ is a threshold value which is chosen according to a suitable trade-off between the attack detection and the false alarm rate.

Remark 1. Define $f(x) = Ax + Bf_n(x)$. When (3) does not have a form of (6), we may choose $\Xi(x)$ as

$$s = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_n \end{bmatrix} = \begin{bmatrix} h_n(x) \\ L_f h_n(x) \\ \vdots \\ L_f^{n-1} h_n(x) \end{bmatrix} = \Xi(x), \tag{10}$$

where $L_f h_n(x)$ is a Lie derivative of $h_n(x)$ along vector field f [27–29].

Remark 2. Unlike linear systems, the observability of the nonlinear system depends on the control input u [27]. Without loss of generality, the system designers will pursue to monitor the system in all regions regardless of u and the

state observer of (7) may realize it. As reported in [24], some papers related to the nonlinear system security have already used the observer, and this paper also follows the common system setting.

3.2. A Multiplicative Coordinated Stealthy Attack. A smart attacker may hope to corrupt the physical plant of (3) without being detected. Defining $\epsilon = y_r - y$ we say that this type of attack has stealthy and effective properties, which is given as follows:

Definition 3. Let $c_T \geq 0$ be a permissible predefined maximum error bound, and δ_T be a detection bound. An attack is called δ_T stealthy and c_T effective, if

$$\|\gamma\| \leq \delta_T, \tag{11}$$

$$\|\epsilon\| = \|y_r - y\| \geq c_T, \tag{12}$$

are satisfied in a steady state [19].

In Definition 3, (11) implies that the attack is not detected by the common anomaly detectors of (7). Also, (12) implies that the attack is effective in the sense of degrading the tracking performance in a steady state. To be more specific, here, ϵ in (12) represents the tracking error occurring due to the attack, and we will call $\mathcal{J}_\epsilon = \|\epsilon\|$ as the attack impact in this paper.

In our attack scenario, several assumptions are required to achieve (11) and (12). The assumptions are described below.

Assumption 2. The nonlinear functions in (3) have homogenous properties given by

$$\begin{aligned} f_n(\Delta_\varepsilon^r x) &= \varepsilon^{\alpha_\omega} f_n(x), \\ g_n(\Delta_\varepsilon^r x) &= \varepsilon^{\beta_\omega} g_n(x), \\ h_n(\Delta_\varepsilon^r x) &= \varepsilon^{\gamma_\omega} h_n(x), \end{aligned} \tag{13}$$

where α_ω, β_ω, γ_ω are the degrees of the homogeneity for $f_n(x)$, $g_n(x)$, and $h_n(x)$ with respect to Δ_ε^r, respectively.

Assumption 3. There exists a Lyapunov function $V(x, c)$ for the stability of the nonlinear feedback control system given by

$$\begin{aligned} \dot{x} &= Ax + B\left(f_n(x) + g_n(x)\right)\mathcal{U}\left(c, h_n(x), 0\right), \\ \dot{c} &= \mathcal{C}\left(c, h_n(x), 0\right). \end{aligned} \tag{14}$$

Assumption 4. The system outputs and control inputs are available to the malicious attackers.

Assumption 5. The reference is not identically zero.

Assumption 6. CPS operates in a steady state during attack period.

Assumption 2 indicates that we only consider the nonlinear systems with homogeneity property. Note that all linear systems always satisfy homogenous property. Assumption 3 indicates that for the feedback system of (3) and (5), the equilibrium point at the origin is asymptotically stable. This may be readily satisfied by the designed tracking controllers. Assumption 4 indicates that the attackers can arbitrarily change control input signals and sensor measurements without any restriction. Assumption 5 indicates that we only consider the cases of nonzero reference. This is a necessary condition for the attack to be effective. Assumption 6 means the attacks may occur in steady state.

Remark 3. Based on Assumption 4, the malicious attackers can inspect the measurements in real time and can know whether Assumption 5 and Assumption 6 are satisfied or not. If the intercepted measurements remain the nonzero constant for a long period, the CPS works in a steady state and the attacks can occur.

Under Assumptions 1, 2, 3, 4, 5, and 6, we introduce the multiplicative coordinated attack posed on the cyber layer. The attack signals selected by attackers take the multiplicative form given by

$$\begin{aligned} \widetilde{u} &= a^u \times u, \\ \widetilde{y} &= a^y \times y, \end{aligned} \tag{15}$$

where a^u and a^y are the attack signals for actuator and sensor, respectively.

Now, using (15), the stealthy condition of a^u and a^y for covertly compromising the nonlinear systems is derived. Let us find the equilibrium points of the nonlinear systems under the attack and attack-free cases. Recall that $a^u = a^y = 1$ is satisfied in attack-free case for all t. We first define an attack-free nonlinear physical system as

$$\begin{aligned} \dot{x}_0 &= Ax_0 + B\left(f_n(x_0) + g_n(x_0)u\right), \\ \widetilde{y}_0 &= y_0 = h_n(x_0), \quad \forall x_0 \in \Omega_x, \end{aligned} \tag{16}$$

where $x_0 = (x_{0,1}, x_{0,2}, \ldots, x_{0,n})^T \in \mathbb{R}^n$ is the plant state, y_0 is the system output, and $\widetilde{y}_0$ is the corrupted system output. Define equilibrium points of x, y, $\widetilde{y}$, x_0, y_0, $\widetilde{y}_0$, and u as $x^\star$, $y^\star$, $\widetilde{y}^\star$, $x_0^\star$, $y_0^\star$, $\widetilde{y}_0^\star$, and $u^\star$, respectively. Then, (3) and (16) are given in a steady state by

$$\begin{aligned} 0_n &= Ax^\star + B\left(f_n(x^\star) + g_n(x^\star)a^u u^\star\right), \\ \widetilde{y}^\star &= a^y y^\star = a^y h_n(x^\star), \\ 0_n &= Ax_0^\star + B\left(f_n(x_0^\star) + g_n(x_0^\star)u^\star\right), \\ \widetilde{y}_0^\star &= y_0^\star = h_n(x_0^\star). \end{aligned} \tag{17}$$

Without loss of generality, for guaranteeing the stealthiness, the received output should have the value identical with the attack-free output, i.e., $\widetilde{y}^\star = \widetilde{y}_0^\star$, and this results in

$$\left(a^y\right)^{\left(\gamma_\omega^{-1}\right)} \Delta_\varepsilon^r x^\star = \Delta_\varepsilon^r x_0^\star. \tag{18}$$

Then, Assumption 2 and (18) yield

$$f_n(\Delta_\varepsilon^r x_0^\star) = f_n\Big((a^y)^{(\gamma_\omega^{-1})}\Delta_\varepsilon^r x^\star\Big) = (a^y)^{(\alpha_\omega\times\gamma_\omega^{-1})} f_n(\Delta_\varepsilon^r x^\star),$$
$$g_n(\Delta_\varepsilon^r x_0^\star) = g_n\Big((a^y)^{(\gamma_\omega^{-1})}\Delta_\varepsilon^r x^\star\Big) = (a^y)^{(\beta_\omega\times\gamma_\omega^{-1})} g_n(\Delta_\varepsilon^r x^\star), \tag{19}$$

and by using (17) and (19), we have

$$0 = f_n(\Delta_\varepsilon^r x^\star) + g_n(\Delta_\varepsilon^r x^\star)a^u u^\star,$$
$$0 = (a^y)^{(\alpha_\omega\times\gamma_\omega^{-1})} f_n(\Delta_\varepsilon^r x^\star) + (a^y)^{(\beta_\omega\times\gamma_\omega^{-1})} g_n(\Delta_\varepsilon^r x^\star)u^\star. \tag{20}$$

Then, (20) yields a relational expression of a^u and a^y given by

$$a^u = (a^y)^{(\beta_\omega-\alpha_\omega)\times\gamma_\omega^{-1}}, \tag{21}$$

and based on this equation, we can present the multiplicative coordinated stealthy attack method for compromising the nonlinear systems with the homogeneity property.

Theorem 1. *Let Assumptions 1, 2, 3, 4, 5, and 6 hold. The stealthy and effective attack for (3) is achieved, if malicious attackers choose*

$$a^u = \kappa,$$
$$a^y = (\kappa)^{-\omega} = (\kappa)^{-\gamma_\omega\times(\alpha_\omega-\beta_\omega)^{-1}}, \tag{22}$$

where $\kappa > 1$ is some positive constant.

Proof. see Appendix A. □

The multiplicative coordinated attack in Theorem 1 has the stealthy property of (11) and the effective property of (12). Now, we quantitatively calculate the attack impact, i.e., $\mathcal{I}_\epsilon$. From Theorem 1, we can find a relation equation in a steady state given by $y = \kappa^\omega \bar{y} = \kappa^\omega y_r$. By using this, $\mathcal{I}_\epsilon$ is finally obtained as

$$\mathcal{I}_\epsilon = \left\| M_\epsilon(\kappa;\omega)\, y_r \right\|, \tag{23}$$

where $M_\epsilon(\kappa;\omega) = 1 - \kappa^\omega$. The attack impact, i.e., $\mathcal{I}_\epsilon$, is proportional to $\|M_\epsilon(\kappa;\omega)\|$, and this is represented in the function determined by the parameters of κ and ω. While ω in $\|M_\epsilon(\kappa;\omega)\|$ is determined by the homogeneous properties of the system, i.e., α_ω, β_ω, γ_ω, the attack design parameter κ is arbitrarily chosen by attackers. As κ is largely chosen under $\omega > 0$, the attack impact, i.e., $\mathcal{I}_\epsilon$, increases accordingly. The property of $M_\epsilon(\kappa;\omega)$ is shown in Figure 1, and it is indeed observed that by choosing large κ, $\|M_\epsilon(\kappa;\omega)\|$ increases. Clearly, the attackers should adjust κ for increasing $\mathcal{I}_\epsilon$, and from the proper selection of κ, the attack impact $\mathcal{I}_\epsilon$ can be made greater than c_T. Here, it should be noted that even if attackers do not have sufficient information about controller (5) and anomaly detector (7), the coordinated attack can be accomplished. Indeed, the attack method of (22) only requires the information on homogeneous degree of physical plant, i.e., α_ω, β_ω, γ_ω.

Remark 4. In a practical view, the attackers may have to consider the saturation of systems [30, 31]. If the attackers have specific information about the permissible input range of the actuator, the attack signal a^u, i.e., $\kappa \in [\underline{\kappa}, \overline{\kappa}]$, should stay in a region given by

$$\frac{\underline{s}}{u^\star} \le \kappa \le \frac{\overline{s}}{u^\star}, \tag{24}$$

where $\underline{s}$ and $\overline{s}$ are the lower and upper limits of the saturating actuator, respectively. Then, $\|\epsilon\|$ is restricted by

$$\|\epsilon\| \le \left\| \max\{M_\epsilon(\kappa;\omega)\} y_r \right\|, \tag{25}$$

for the admissible range of κ in (24).

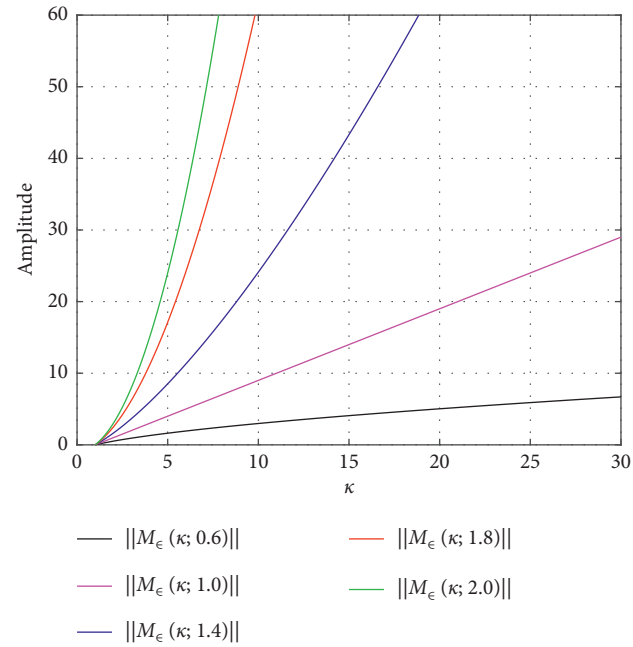


Figure 1: $\|M_\epsilon(\kappa;\omega)\|$ over κ for several values of ω.

Corollary 1. *Let Assumptions 1, 2, 3, 4, 5, and 6 hold. If the control input stays in zero, malicious attackers can choose a stealthy and effective attack signal as*

$$a^y = \nu, \tag{26}$$

where ν is some constant.

Proof. see Appendix B. □

The method in Corollary 1 implies that the attackers may compromise (3) only by using the output signal without any needs of the control input signal. The attackers can only use the single communication channel (output channel), and this relieves Assumption 4. Also, in the creation of the attack signal, the homogenous properties, i.e., ω, are not used. This means that the riskiness of the attack can be increased in that the attackers do not need the system model knowledge. If the target system is linear and has one or more poles at the original point of $\mathbf{s}$-domain, the attacker may use Corollary 1.

It is worth noting that the stealthy attack technique for the linear systems can also be verified from Theorem 1. We define the linear system as

$$\begin{aligned} \dot{x} &= A_P x + B_P \widetilde{u}, \\ y &= C_P x, \end{aligned} \tag{27}$$

where A_P, B_P, and C_P are the matrices with appropriate dimensions. By following the canonical form of (3), the functions of (27) can be represented by

$$\begin{aligned} f_n(x) &= \sum_{i=1}^{n} a_i x_i, \\ g_n(x) &= b, \\ h_n(x) &= \sum_{j=1}^{n} c_j x_j, \end{aligned} \tag{28}$$

where a_i for all i, b, and c_j for all j are some constants. The homogeneity degrees of (28) satisfy $\alpha_\omega = \gamma_\omega$ and $\beta_\omega = 0$ with respect to Δ_ϵ^r, which yields $\omega = \gamma_\omega \times (\alpha_\omega - \beta_\omega)^{-1} = \gamma_\omega \times (\gamma_\omega)^{-1} = 1$. Therefore, from Theorem 1, the attack signals should be chosen as $a^u = \kappa$ and $a^y = \kappa^{-1}$, and we can propose Corollary 2 as the method for stealthily compromising the linear systems.

Corollary 2. *Let Assumptions 1, 3, 4, 5, and 6 hold. The stealthy and effective attack for linear systems in (27) is achieved, if malicious attackers choose*

$$\begin{aligned} a^u &= \kappa, \\ a^y &= \frac{1}{\kappa}, \end{aligned} \tag{29}$$

where $\kappa > 1$ is some constant value.

Proof. see [19] for more detailed proof. □

When the attackers compromise the linear systems, any model knowledge about the system dynamics is not required. However, for the stealthy attacks of the nonlinear systems, the attackers may need the minimum knowledge of homogeneity degrees in the nonlinear dynamics.

Until now, we presented the attack methods for the specific systems which have the forms of (3) and (27). However, rigorously, Theorem 1 and Corollary 2 do not confine the attack targets into the specific systems of (3) and (27). This means if a target system can be changed into the forms of (3) and (27), the stealthy attack may be achieved. In other words, if there exists new state variable $\zeta \in \mathbb{R}^n$ given by

$$\zeta = \Phi(x), \tag{30}$$

where $\Phi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ is a diffeomorphism function such that the system transformed has the forms of (3) or (27), the stealthy attack can be achieved. Here, it should be pointed out that if the attackers use the coordinate changes of (30), considerable model knowledge may be required compared with the existing methods proposed in Theorem 1 and Corollary 2. The additional description will be proposed in the simulation of Section 4.

It is worth noting that the multiplicative coordinated stealthy attack may not be easily detected by the existing watermarking detection methods. This is because the response of the probing signals can be obtained without any modification under the attack. Comparing with the replay attacks being easily detected by the probing signals [12, 13], the coordinated attack methods are much dangerous. The additional description will be also presented in Section 4.

From attacker's perspective, we introduce several efficient attack methods. Below is, for the nonlinear systems, the extended version of the linear attack method introduced in [19].

Remark 5. When the attacks occur, the abrupt changes of the control input and system output may incur the poor transient performance such as the peaking phenomenon of undershoot or overshoot [32]. This means that the stealthiness can be hindered at the initial time of attack. As a remedy, we introduce the attack method that can guarantee the transient performance as

$$\begin{aligned} a^u &= \kappa, \\ a^y &= L(\mathbf{s})(\kappa)^{-\omega}, \end{aligned} \tag{31}$$

where $L(\mathbf{s})$ is the stable low-pass filter with unity dc-gain.

Remark 6. In order to destroy the nonlinear systems (3), the attackers may hope to employ the increasing time-varying signals, i.e., $\dot{a}^u > 0$. The attack may be achieved, if $a^u \geq 1$ is slowly increasing such that

$$0_n \approx Ax + B\left(f_n(x) + g_n(x)\widetilde{u}\right), \tag{32}$$

is satisfied.

4. Examples

4.1. Example 1. In this section, we conduct various simulations and study the multiplicative coordinated stealthy attack. Let us consider a nonlinear forced physical system given by

$$\begin{aligned} \dot{x} &= \begin{bmatrix} x_2 \\ -4x_1^3 - 3x_1^2 x_2 \end{bmatrix} + \begin{bmatrix} 0 \\ 2 \end{bmatrix} \widetilde{u}, \\ y &= x_1, \quad \forall x \in \mathbb{R}^2, \end{aligned} \tag{33}$$

where $x(0) = (0,0)^T$. For following a desired reference $y_r = 1$, we design a feedback linearized tracking controller introduced in [33] as

$$u = 2z_1^3 + 1.5z_1^2 z_2 - 5\dot{\widetilde{y}} - 12.5\widetilde{y} + 12.5y_r, \tag{34}$$

where $z = (z_1, z_2)^T \in \mathbb{R}^2$. The nonlinear observer in the anomaly detector is designed as

$$\begin{aligned} \dot{z} &= \begin{bmatrix} z_2 \\ -4z_1^3 - 3z_1^2 z_2 \end{bmatrix} + \begin{bmatrix} 0 \\ 2 \end{bmatrix} u - \begin{bmatrix} 6 \\ 9 \end{bmatrix} \gamma, \\ \widehat{y} &= z_1. \end{aligned} \tag{35}$$

The homogeneous degrees of (33) are determined as $\alpha_\omega = 3$, $\beta_\omega = 0$, and $\gamma_\omega = 1$ with respect to $\Delta_\epsilon^{\{1,1\}}$. We assume that the attackers who aspire to corrupt (33) choose the attack signals as

$$a^u = 5.4,$$
$$a^y = \frac{5}{\mathbf{s}+5} \times (5.4)^{-1/3}, \tag{36}$$

for $t \in [50, 150]$.

The simulation results are shown in Figure 2. The output signal, the corrupted output signal, and the residue signal are shown in Figures 2(a)–2(c), respectively. Before the attack, it is observed that the output signal in Figure 2(a) follows the reference. However, after the attack, due to the attack signals injected into the target system, the actual plant output does not track the reference. The attack impact occurs in control system. The received system output in Figure 2(b) seems as if the output signal asymptotically follows the reference. The anomaly detector which receives the corrupted output signal does not trigger the alarm. Indeed, as shown in Figure 2(c), the residue signal does not exceed the threshold value. From the results, we can claim that the attack has effective and stealthy properties.

For the system of (33)–(36), calculating the attack impacts over several attack signals κ may be worthy work. The result is illustrated in Figure 3. The attack impact is calculated as 0.7544, which is identical with the size of the tracking error shown in Figure 2(a).

In this simulation, it needs to be emphasized that the attackers may have imprecise model knowledge about (33) as

$$\begin{aligned} f_n(x) &= \tilde{m}_1 x_1^3 + \tilde{m}_2 x_1^2 x_2, \\ g_n(x) &= \tilde{m}_3, \\ h_n(x) &= \tilde{m}_4 x_1 + \tilde{m}_5 x_2, \end{aligned} \tag{37}$$

where $\tilde{m}_i$ for $i = 1, 2, \ldots, 5$ are uncertain parameters. However, even if the attackers have the uncertain parameters, the attack signal in (36) can be formulated.

4.2. Example 2. In this section, we show that the multiplicative coordinated stealthy attack may be more dangerous than the replay attack. For the demonstration, the nonlinear system of (33) is considered again and we assume that probing signals p^w is combined with the desired reference $y_r = 1$. The probing signals are selected as various sine waves with different amplitudes over time interval. The new reference denoted by y_r^w is given by

$$\begin{aligned} y_r^w &= y_r + p^w \\ &= \begin{cases} 0, & t \in [0, 3), \\ 1 + 0.10 \sin(0.5(t-3)), & t \in [3, 60), \\ 1 + 0.15 \sin(0.5(t-3)), & t \in [60, 110), \\ 1 + 0.05 \sin(0.5(t-3)), & t \in [110, 150]. \end{cases} \end{aligned} \tag{38}$$

We design a controller capable for tracking y_r^w as

$$u = 2z_1^3 + 1.5 z_1^2 z_2 - 5\dot{\tilde{y}} - 12.5\tilde{y} + 0.5\ddot{y}_r^w + 5\dot{y}_r^w + 12.5 y_r^w. \tag{39}$$

The anomaly detector identical with (35) is used in this simulation. In order to show the generation of various attack signals, we assume that the attack signals for corrupting (33) are slowly varying as

$$\begin{aligned} a^u &= \left(8 \times 10^{-4} \frac{t^3}{t+50} \right), \\ a^y &= \left(8 \times 10^{-4} \frac{t^3}{t+50} \right)^{-1/3}, \end{aligned} \tag{40}$$

for $t \in [50, 150]$.

The results are shown in Figure 4. Unlike the replay attack, the corrupted output reacts to the watermarking signals although the attack occurs.

For clarity, we show the simulation result for the replay attack. It is assumed that the output is recorded from 20 s until 80 s for the replay attack and the recorded output is injected after 90 s. As expected, the recorded output shown in Figure 5 does not respond to the watermarking signals. Through the simulation, the riskiness of the coordinated attack is definitely highlighted.

In addition, we conduct comparison with the false data injection (sensor) attack [14, 15] by simulations. The system considered is the same as before, and we choose the sensor attack signal a^y as

$$a^y = \frac{1.5}{\mathbf{s}+1.5} \times (3.5), \tag{41}$$

and it is assumed to be added into y after 50 s, i.e., $\tilde{y} = y + a^y$. The simulation results are shown in Figure 6. As expected, the false data injection attack renders the corrupted output deviate from the desired reference. Unlike the multiplicative coordinated attack, the false data injection attack is easily detected by the anomaly detector. Hence, the potential danger posed by the multiplicative coordinated attack is illustrated.

4.3. Example 3. Consider a nonlinear system given by

$$\begin{aligned} \dot{x} &= \begin{bmatrix} -9x_1 + 5x_2^3 \\ -2x_1 x_2^{-2} + \frac{1}{3} x_2 \end{bmatrix} + \begin{bmatrix} 1 \\ \frac{1}{3} x_2^{-2} \end{bmatrix} \tilde{u}, \\ y &= x_1 - x_2^3, \quad \forall x \in \Omega_x, \end{aligned} \tag{42}$$

where $\Omega_x = \{x \in \mathbb{R}^2 : x_1 \geq 0.4,\ x_2 \geq 0.5\}$ and $x(0) = (1, 1)^T$.

The nonlinear system in (42) does not follow the specific form of (3) and (27). The attackers may not cause severe damage in the system of (42) using methods of Theorem 1 and Corollary 2. However, from the specific coordinate transformation, the smart attackers may find the new fact that (42) can be a target system. Define a new state variable $\zeta = (\zeta_1, \zeta_2)^T \in \mathbb{R}^2$ as $\zeta_1 = x_1 - x_2^3 = \Phi_1(x)$ and $\zeta_2 = x_2^3 = \Phi_2(x)$. Then, we have a linear system given by

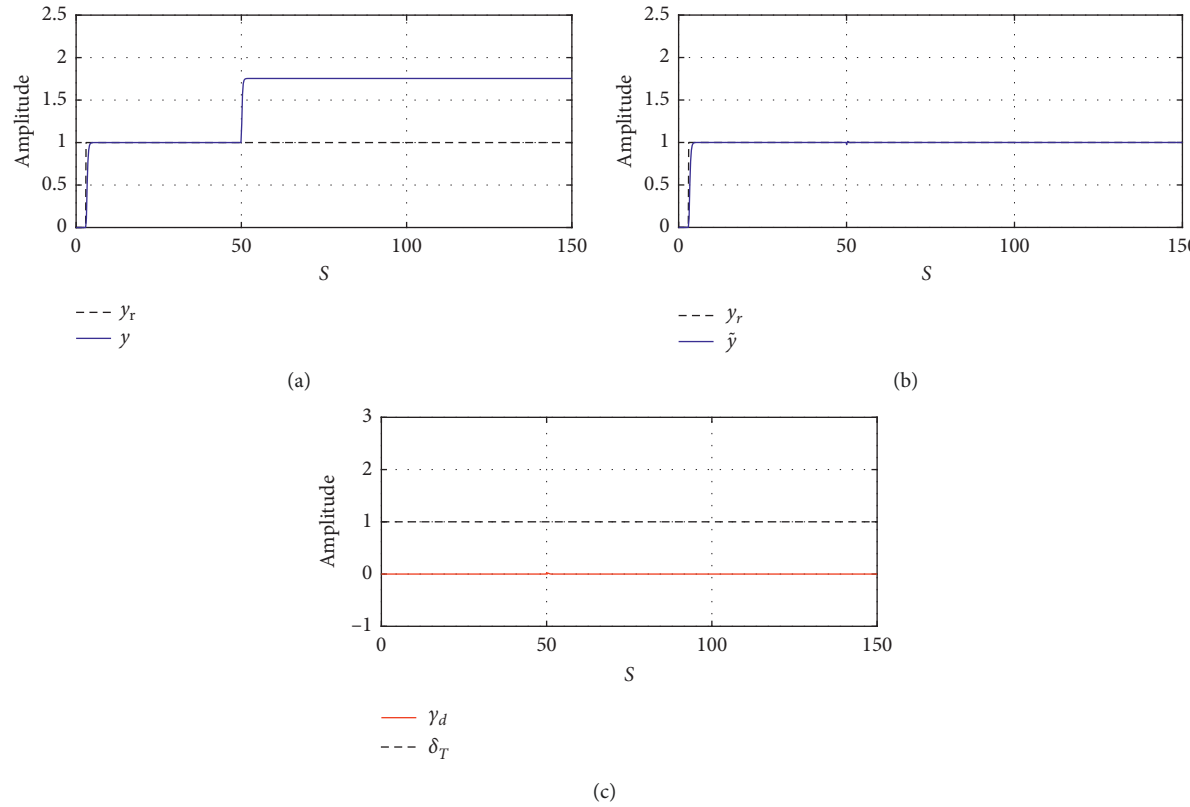


Figure 2: Simulation results of (33)–(36). (a) Reference and system output. (b) Reference and corrupted output. (c) Residue signal.

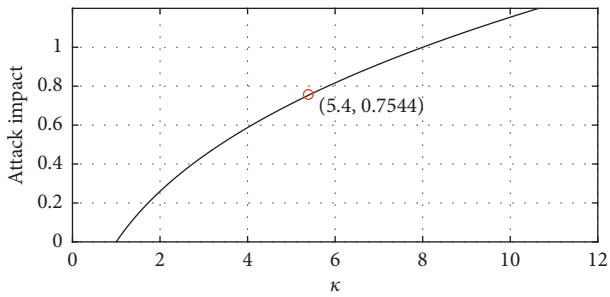


Figure 3: Attack impacts $\mathcal{J}_\epsilon$ over several κ.

$$\dot{\zeta} = \begin{bmatrix} -3 & 1 \\ -6 & -5 \end{bmatrix} \zeta + \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tilde{u}, \qquad y = \zeta_1. \tag{43}$$

Now, the attackers can compromise (42) from Corollary 2. This clearly shows that the multiplicative coordinated attack can be applied into various nonlinear systems. We show that the multiplicative coordinated stealthy attack in Corollary 2 can make the system states of (42) far away from the desired trajectories with the stealthiness. The simulation results are obtained by setting $u^\star$ as a constant. The system states, the system output, and the corrupted system output are illustrated in Figure 7. The system states $x_1^\star$ and $x_2^\star$ for $\kappa \in [1, 10]$ are shown in Figure 7(a). As κ increases, the system states gradually deviate with the nonlinear nature from the desired trajectories, i.e., $x^\star$ when $\kappa = 1$. While the actual system output $y^\star$ varies for κ, the corrupted output $\tilde{y}^\star$ remains steady, as shown in Figure 7(b). The effectiveness is validated.

Remark 7. It is worth noting that in order to demonstrate the effectiveness of the attack, the experiment using a quadrotor called AR-drone was conducted in [19]. For more detailed description, see [19].

5. Discussion for Detection Methods

Although this paper mainly focuses on how to formulate the attack signals, proposing detection methods for multiplicative coordinated stealthy attack can be worthy work. In this section, we briefly suggest two detection methods using smart sensors and eliminating homogeneous properties.

5.1. Use Smart Sensors. Using a detection method introduced in [19] may be a solution for detecting the coordinated attacks in the nonlinear systems. Although the detection method has been developed for the linear systems, it seems to be applicable to the nonlinear systems. The detection method proposed in [19] follows design procedure below:

(1) Before transmitting the sensor measurements y, the smart sensor with calculation capability adds secret nonzero values χ to the sensor measurements

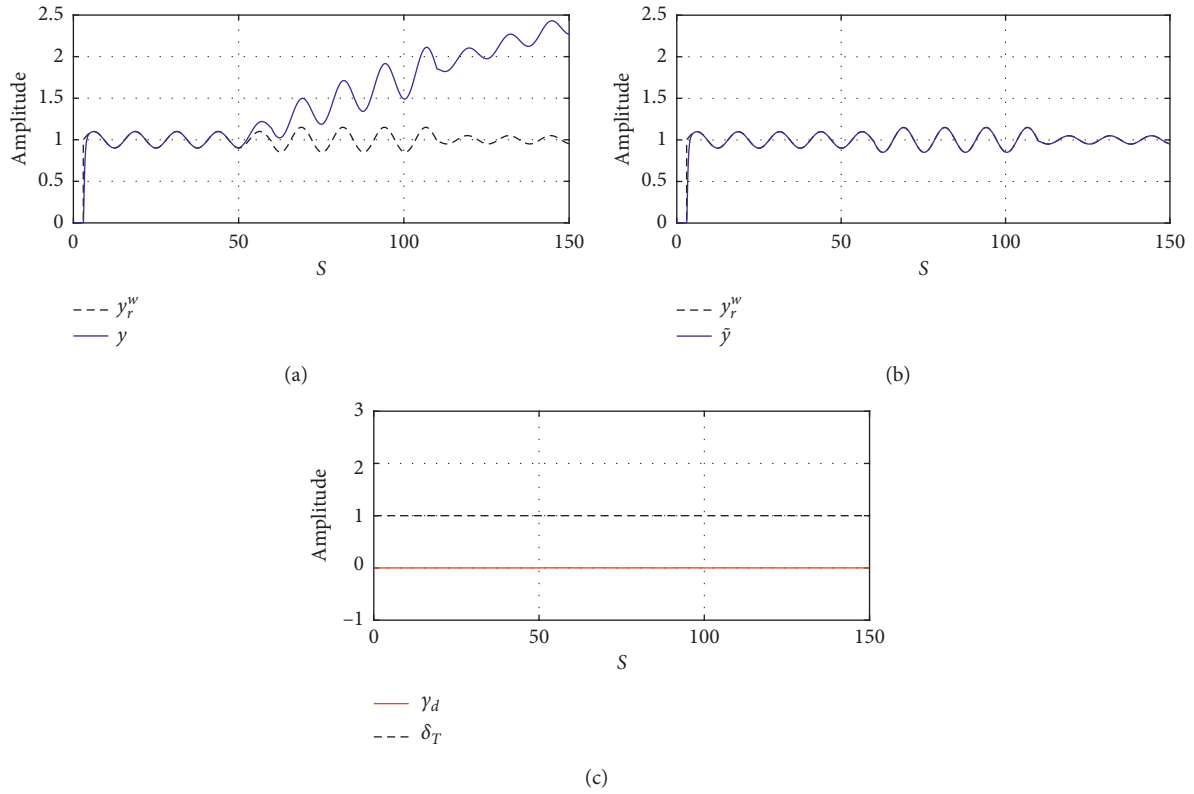


Figure 4: Simulation results of (33)–(36). (a) Reference and system output. (b) Reference and corrupted output. (c) Residue signal.

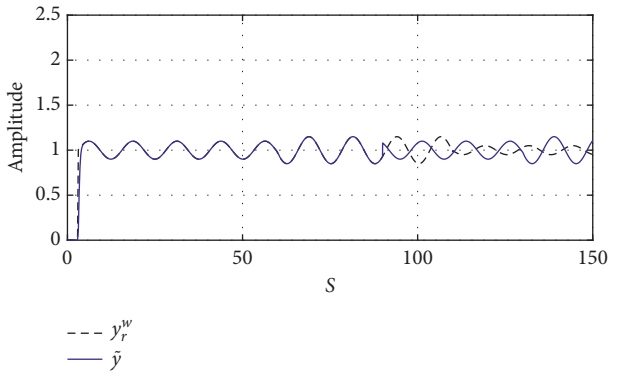


Figure 5: Simulation result of replay attack.

(2) After the transmission, data receivers construct the transmitted signal for securing original signal by subtracting χ

For clarity, we mathematically represent the transmitted signal y_T and the constructed signal y_C as

$$\begin{aligned} y_T &= y + \chi, \\ y_C &= \tilde{y} - \chi. \end{aligned} \tag{44}$$

If the multiplicative coordinated attack does not occur, the receiver secures the original signal, i.e.,

$$y_C = y_T - \chi = y = y_0. \tag{45}$$

However, when the transmitted signal y_T is modified by the coordinated attacks, the constructed signal y_C is changed into

$$y_C = \kappa^{-\omega} y + (\kappa^{-\omega} - 1)\chi = \kappa^{-\omega} y + H(\kappa; \omega; \chi), \tag{46}$$

and this shows that the attackers may not accomplish the stealthy attacks because of the new term, i.e., $H(\kappa; \omega; \chi)$. Here, it should be noted that $H(\kappa; \omega; \chi)$ affects the residue signal and as the system designers choose large χ, the new term, i.e., $H(\kappa; \omega; \chi)$, increases accordingly. Indeed, we can show that

$$\|H(\kappa; \omega; \chi_1)\| > \|H(\kappa; \omega; \chi_2)\| \tag{47}$$

holds for $\chi_1 > \chi_2$. If the system designers hope to detect the attack, χ needs to be chosen as large value.

5.2. Eliminate Homogeneous Properties. Eliminating homogeneous properties may become another detection method. We propose modifying system dynamics by augmenting new nonlinear dynamics which the attackers do not cognize with (3). This may be realized by connecting the new nonlinear systems into (3) as a parallel way. For clear description, we define the modified nonlinear system as

$$\begin{aligned} \dot{q} &= \mathscr{A} q + \mathscr{B}(f_v(q) + g_v(q)\tilde{u}), \\ y &= h_v(q), \end{aligned} \tag{48}$$

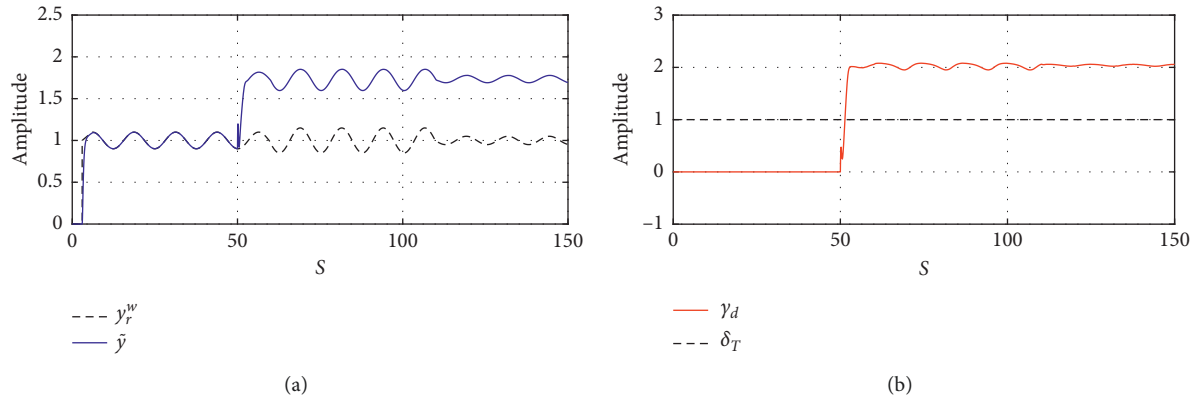


Figure 6: Simulation results of false data injection attack. (a) Reference and corrupted output. (b) Residue signal.

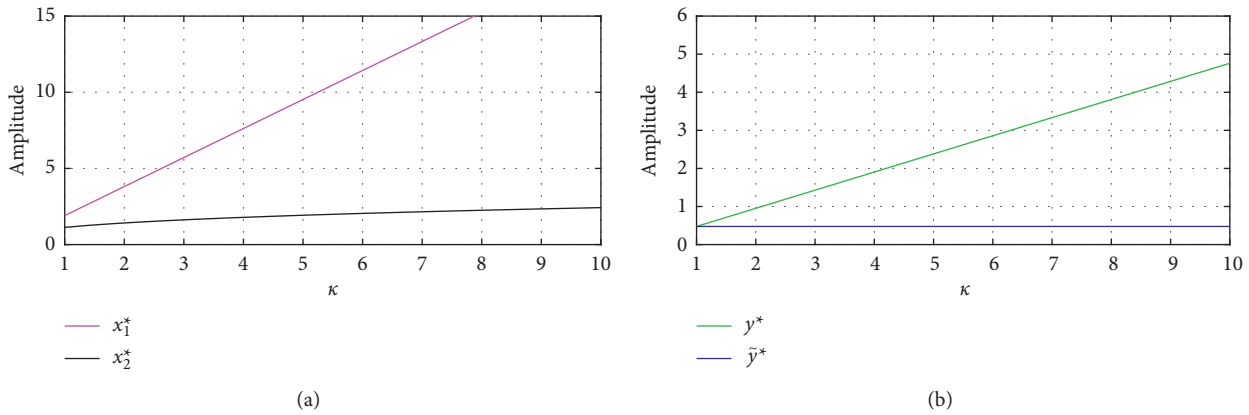


Figure 7: Simulation results of (42)-(43). (a) System states over several κ in a steady state. (b) System output and corrupted output over several κ in a steady state.

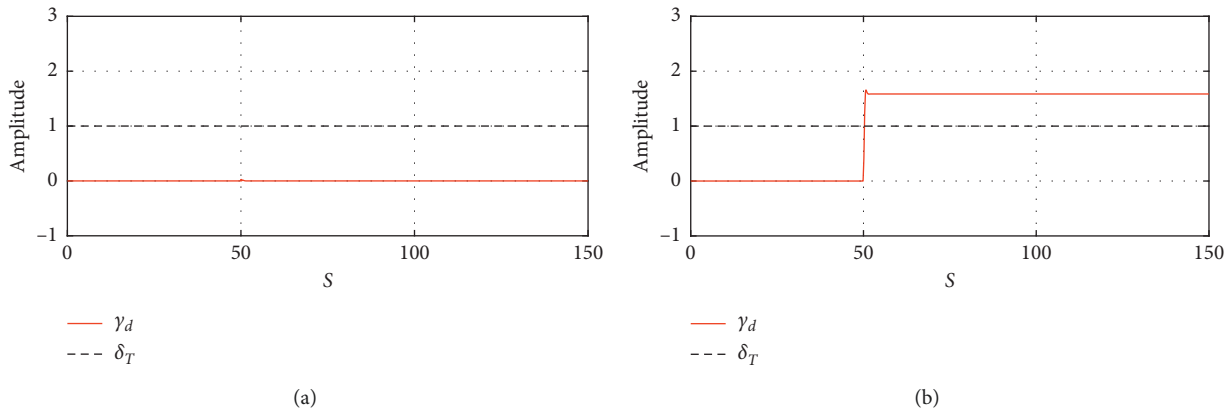
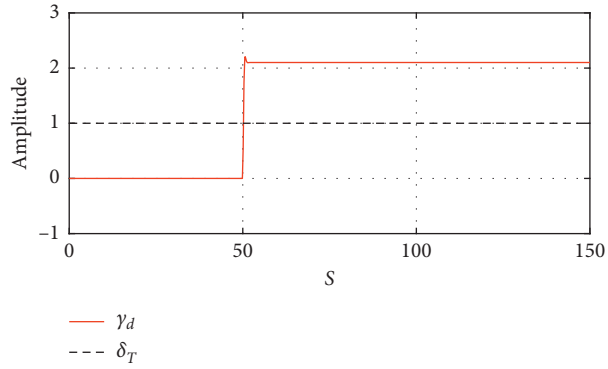
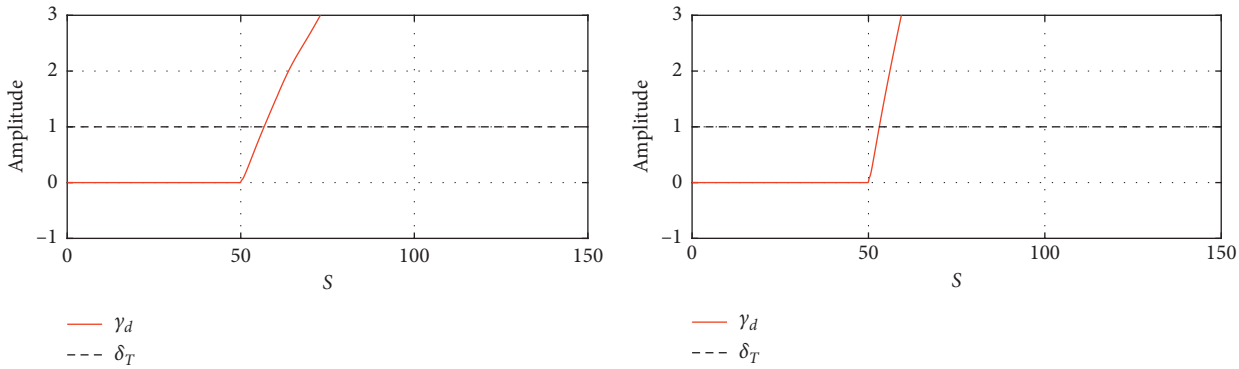


Figure 8: Continued.



(c)

Figure 8: Attack detection results for several χ in systems of Example 1. (a) Residue signal for $\chi = 0$. (b) Residue signal for $\chi = 7$. (c) Residue signal for $\chi = 9$.



(a) (b)

Figure 9: Attack detection results for several χ in systems of Example 2. (a) Residue signal for $\chi = 20$. (b) Residue signal for $\chi = 40$.

where $f_v(\cdot)$, $g_v(\cdot)$, and $h_v(\cdot)$ are smooth mapping functions, $q \in \mathbb{R}^v$ is new state with $v > n$, and the matrices $\mathscr{A}$ and $\mathscr{B}$ are defined as

$$\mathscr{A} = \begin{bmatrix} 0_{v-1} & I_{v-1} \\ 0 & 0_{v-1}^T \end{bmatrix} \in \mathbb{R}^{v \times v}, \qquad \mathscr{B} = \begin{bmatrix} 0_{v-1} \\ 1 \end{bmatrix} \in \mathbb{R}^v. \tag{49}$$

If the system designers can reconfigure (3) as a system without homogeneous characteristics, i.e.,

$$\begin{aligned} f_v(\Delta_\varepsilon^r q) &\neq \varepsilon^{\alpha_\omega} f_v(q), \\ g_v(\Delta_\varepsilon^r q) &\neq \varepsilon^{\beta_\omega} g_v(q), \\ h_v(\Delta_\varepsilon^r q) &\neq \varepsilon^{\gamma_\omega} h_v(q), \end{aligned} \tag{50}$$

the attackers may not accomplish the stealthy attack clearly.

Now, we validate the effectiveness of the detection method using smart sensors and consider the systems of Example 1 again. We conduct simulations for several χ, and the results are obtained in Figure 8. In the case when the proposed detection method is not applied, i.e., $\chi = 0$, the anomaly detector cannot detect the attack. However, when the detection method is employed, i.e., $\chi = 7, 9$, the anomaly detector detects the attack as shown in Figures 8(b) and 8(c). The results applying the proposed method in Example 2 are shown in Figure 9. As displayed in Figure 8, we can observe that the coordinated attack is detected. The effectiveness of the proposed method is clearly demonstrated. The detailed analysis for the detection methods will be considered as a future work, and we expect that using smart sensors and eliminating homogeneous properties by modifying system dynamics become appropriate solutions for the attack detection.

6. Conclusions

The multiplicative coordinated stealthy attack was developed for corrupting the homogeneous nonlinear systems. We analyzed the attack and validated the dangerousness through several simulations. Also, the detection methods were briefly discussed. We hope that the current research results would help to CPS security.

Limits of current study are summarized as follows. This paper only considers single input single output nonlinear systems. Extending the multiplicative coordinated attacks into multiple input multiple output dynamics will be future work. Finally, although this work conceives a method of

attack design, discussions on countermeasures are limited. A more comprehensive detection method will be necessary.

Appendix

A. Proof of Theorem 1

We show that (22) satisfies the stealthy property. The transformed nonlinear system (6) under attack is given by

$$\dot{s} = \begin{bmatrix} \dot{s}_1 \\ \dot{s}_2 \\ \vdots \\ \dot{s}_n \end{bmatrix} = \begin{bmatrix} s_2 \\ s_3 \\ \vdots \\ \alpha_n(s) \end{bmatrix} + \begin{bmatrix} \beta_1(s_1) \\ \beta_2(s_1, s_2) \\ \vdots \\ \beta_n(s) \end{bmatrix} \kappa u, \qquad \widetilde{y} = (\kappa)^{-\omega} C s. \tag{A.1}$$

Define $\widetilde{s} = (\kappa)^{-\omega} s$. Then,

$$\dot{\widetilde{s}} = \begin{bmatrix} \widetilde{s}_2 \\ \widetilde{s}_3 \\ \vdots \\ (\kappa)^{-\omega} \alpha_n(\kappa^{\omega} \widetilde{s}) \end{bmatrix} + \begin{bmatrix} (\kappa)^{1-\omega} \beta_1(\kappa^{\omega} \widetilde{s}_1) \\ (\kappa)^{1-\omega} \beta_2(\kappa^{\omega} \widetilde{s}_1, \kappa^{\omega} \widetilde{s}_2) \\ \vdots \\ (\kappa)^{1-\omega} \beta_n(\kappa^{\omega} \widetilde{s}) \end{bmatrix} u, \qquad \widetilde{y} = C \widetilde{s}. \tag{A.2}$$

Define estimation error as $e = z - \widetilde{s}$. Then, the estimation error dynamics is represented by

$$\dot{e} = Ae + \Gamma(z, \widetilde{s}, u) - P^{-1} C^T C e, \tag{A.3}$$

where $\Gamma_i(z, \widetilde{s}, u)$ for $1 \le i \le n$ is defined as

$$\begin{aligned} \Gamma_1 &= \beta_1(z_1) u - (\kappa)^{1-\omega} \beta_1(\kappa^{\omega} \widetilde{s}_1) u, \\ \Gamma_2 &= \beta_2(z_1, z_2) u - (\kappa)^{1-\omega} \beta_2(\kappa^{\omega} \widetilde{s}_1, \kappa^{\omega} \widetilde{s}_2) u, \\ &\vdots \\ \Gamma_n &= \alpha_n(z) - (\kappa)^{-\omega} \alpha_n(\kappa^{\omega} \widetilde{s}) + \beta_n(z) u - (\kappa)^{1-\omega} \beta_n(\kappa^{\omega} \widetilde{s}) u. \end{aligned} \tag{A.4}$$

The following proof is based on [34]. Let us define $\xi = \Lambda e$, where $\Lambda \coloneqq \mathrm{diag}(1, (1/\theta), \ldots, (1/\theta^{n-1})) \in \mathbb{R}^{n \times n}$. By Assumption 1 and boundedness of the control input, we set $\overline{M}_i$ for $1 \le i \le n$ such that $\theta^{1-i} |\Gamma_i| < \overline{M}_i \|\xi\|$ is satisfied. Then, $\|\Lambda \Gamma\| \le \overline{M} \|\xi\|$, where

$$\overline{M} = n \times \max\{\overline{M}_1, \overline{M}_2, \ldots, \overline{M}_n\}. \tag{A.5}$$

By choosing an unique positive definite solution $\widetilde{P}$ satisfying $0_{n \times n} = -\dot{\widetilde{P}} - \widetilde{P} A - A^T \widetilde{P} + C^T C$, we can derive a dynamics of ξ as $\dot{\xi} = \theta A \xi + \Lambda \Gamma - \theta \widetilde{P}^{-1} C^T C \xi$. The time derivative of $\xi^T \widetilde{P} \xi$ is given by

$$\begin{aligned} \frac{d}{dt}\left(\xi^T \widetilde{P} \xi\right) &= -\theta \xi^T \widetilde{P} \xi - \theta \xi^T C^T C \xi + 2 \xi^T \widetilde{P} \Lambda \Gamma \le -\theta \underline{\mu} \|\xi\|^2 \\ &\quad + 2 \overline{\mu} \|\xi\| \|\Lambda \Gamma\| \le -\theta \underline{\mu} \|\xi\|^2 + 2 \overline{\mu} \overline{M} \|\xi\|^2, \end{aligned} \tag{A.6}$$

where $\underline{\mu}$ and $\overline{\mu}$ are minimum and maximum eigenvalue of $\widetilde{P}$. By choosing $\theta > 1$, we have

$$\|z(t) - \widetilde{s}(t)\| \le \overline{w} \eta(\theta) \exp\left(-\frac{\theta t}{4}\right) \|e(0)\|, \tag{A.7}$$

where $\eta(\theta)$ is a nondecreasing function and $\overline{w}$ is some positive constant. The inequality (A.7) guarantees $\|z(t) - \widetilde{s}(t)\| \longrightarrow 0$, i.e., $\|\widehat{y}(t) - \widetilde{y}(t)\| \longrightarrow 0$. The stealthiness is guaranteed in a steady state.

Next, we show that (22) satisfies the effective property. In a steady state, y is identical with $\kappa^{\omega} y_r$. By definition of $\|\epsilon\|$, we can derive

$$\|\epsilon\| = \left\| y_r - \kappa^{\omega} y_r \right\| = \left\| (1 - \kappa^{\omega}) y_r \right\|. \tag{A.8}$$

This shows that choosing proper κ makes $\|\epsilon\| > c_T$. The effectiveness is guaranteed.

B. Proof of Corollary 1

Since input signal is zero in a steady state, we have, from (20),

$$0 = f_n(\Delta_{\varepsilon}^r x^*). \tag{B.1}$$

This shows that no stealthy condition is formulated for x^*. Therefore, the sensor attack signal a^y can be arbitrarily selected.

Data Availability

The data used to support the findings of this study are included within the article.

Disclosure

A preliminary version of this manuscript, i.e., [19], was presented in IEEE Conference on Control Technology and Applications (CCTA 2018). Unlike the preliminary version focusing on linear systems, current version includes new results obtained from the extension of nonlinear systems.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was partly supported by the Institute for Information and Communications Technology Promotion (IITP) grant funded by the Korea government (MSIP) (2014-0-00065, Resilient Cyber-Physical Systems Research) and partly supported by the Global Research Laboratory Program through the National Research Foundation of Korea (NRF-2013K1A1A2A02078326). This work was also supported by the DGIST R&D Programs of the Ministry of Science and ICT (18-ST-02 and 18-EE-01).

References

[1] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," in *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops*, pp. 495–500, Beijing, China, June 2008.

[2] E. A. Lee, "Cyber physical systems: design challenges," in *Proceedings of the IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC)*, pp. 363–369, Orlando, FL, USA, May 2008.

[3] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, vol. 80, no. 5, pp. 973–993, 2014.

[4] J. Slay and M. Miller, "Lessons learned from the Maroochy Water Breach," in *Critical Infrastructure Protection*, pp. 73–82, Springer, Boston, MA, USA, 2007.

[5] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *Proceedings of the 37th Annual Conference of the IEEE Industrial Electronics Society (IECON)*, pp. 4490–4494, Melbourne, Australia, November 2011.

[6] G. Na, D. Seo, and Y. Eun, "Methods of state estimation resilient against sensor attacks and robust against exogenous disturbances," in *Proceedings of the IEEE Conference on Control Technology and Applications (CCTA)*, pp. 1300–1305, Hawaii, HI, USA, August 2017.

[7] H. Jeon, S. Aum, H. Shim, and Y. Eun, "Resilient state estimation for control systems using multiple observers and median operation," *Mathematical Problems in Engineering*, vol. 2016, Article ID 3750264, 9 pages, 2016.

[8] M. Pajic, J. Weimer, N. Bezzo et al., "Robustness of attack-resilient state estimators," in *Proceedings of the ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, pp. 163–174, Berlin, Germany, April 2014.

[9] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using Kalman filter," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 4, pp. 370–379, 2014.

[10] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[11] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni, "Analysis of a denial of service attack on TCP," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 208–223, Oakland, CA, USA, May 1997.

[12] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proceedings of the 47th Annual Allerton Conference*, pp. 911–918, Monticello, IL, USA, September 2009.

[13] A. Hoehn and P. Zhang, "Detection of replay attacks in cyber-physical systems," in *Proceedings of the IEEE American Control Conference*, pp. 290–295, Boston, MA, USA, July 2016.

[14] Y. Huang, M. Esmalifalak, H. Nguyen et al., "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 27–33, 2013.

[15] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[16] G. Park, H. Shim, C. Lee, Y. Eun, and K. H. Johansson, "When adversary encounters uncertain cyber-physical systems: robust zero-dynamics attack with disclosure resources," in *Proceedings of the IEEE 55th Conference on Decision and Control*, pp. 5085–5090, Las Vegas, NV, USA, December 2016.

[17] H. Jeon and Y. Eun, "A stealthy sensor attack for uncertain cyber-physical systems," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6345–6352, 2019.

[18] Z. Li and G. H. Yang, "A data-driven covert attack strategy in the closed-loop cyber-physical systems," *Journal of the Franklin Institute*, vol. 355, no. 14, pp. 6454–6468, 2018.

[19] G. Na and Y. Eun, "A multiplicative coordinated stealthy attack and its detection for cyber physical systems," in *Proceedings of the IEEE Conference on Control Technology and Applications (CCTA)*, pp. 1698–1703, Copenhagen, Denmark, August 2018.

[20] N. Nakamura, H. Nakamura, Y. Yamashita, and H. Nishitani, "Homogeneous stabilization for input affine homogeneous systems," *IEEE Transactions on Automatic Control*, vol. 54, no. 9, pp. 2271–2275, 2009.

[21] C. Qian, "A homogeneous domination approach for global output feedback stabilization of a class of nonlinear systems," in *Proceedings of the IEEE American Control Conference*, pp. 4708–4715, Portland, ON, USA, June 2005.

[22] A. Anta and P. Tabuada, "Self-triggered stabilization of homogeneous control systems," in *Proceedings of the IEEE American Control Conference*, pp. 4129–4134, Seattle, WA, USA, June 2008.

[23] T. Yang, C. Murguia, M. Kuijper, and D. Nesic, "Attack detection and isolation for discrete time nonlinear systems," 2018, https://arxiv.org/abs/1806.06484.

[24] J. Kim, C. Lee, H. Shim, Y. Eun, and J. H. Seo, "Detection of sensor attack and resilient state estimation for uniformly observable nonlinear systems having redundant sensors," *IEEE Transactions on Automatic Control*, vol. 64, no. 3, pp. 1162–1169, 2018.

[25] W. Zhang, Z. Wang, Y. Liu, D. Ding, and F. E. Alsaadi, "Sampled-data consensus of nonlinear multiagent systems subject to cyber attacks," *International Journal of Robust and Nonlinear Control*, vol. 28, no. 1, pp. 53–67, 2018.

[26] W. Hahn, *Stability of Motion*, Springer Verlag, Berlin, Germany, 1967.

[27] J. P. Gauthier and G. Bornard, "Observability for any $u(t)$ of a class of nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 26, no. 4, pp. 992–926, 1981.

[28] J. P. Gauthier, H. Hammouri, and S. Othman, "A simple observer for nonlinear systems applications to bioreactors," *IEEE Transactions on Automatic Control*, vol. 37, no. 6, pp. 875–880, 1992.

[29] G. Besancon, "Nonlinear observers and applications," in *Lecture Notes in Control and Information Science*, vol. 363, Springer Verlag, Berlin, Germany, 2007.

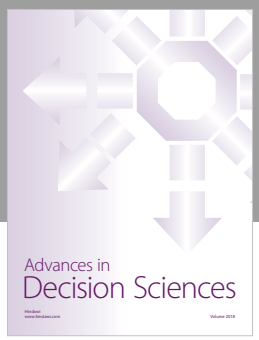
[30] Y. Eun, P. T. Kabamba, and S. M. Meerkov, "System types in feedback control with saturating actuators," *IEEE Transactions on Automatic Control*, vol. 49, no. 2, pp. 287–291, 2004.

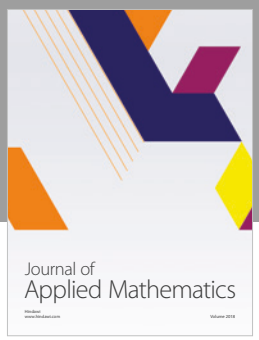
[31] S. Ching, Y. Eun, C. Gokcek, P. T. Kabamba, and S. M. Meerkov, *Quasilinear Control: Performance Analysis and Design of Feedback Systems with Nonlinear Sensors and Actuators*, Cambridge University Press, Cambridge, UK, 2010.

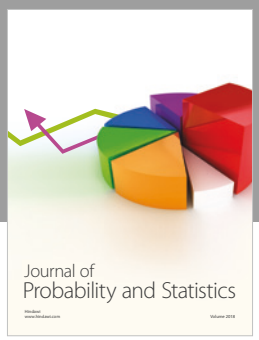
[32] H. J. Sussmann and P. V. Kokotovic, "The peaking phenomenon and the global stabilization of nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 36, no. 4, pp. 424–440, 1991.

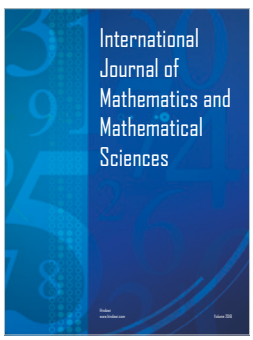
[33] J. J. E. Slotine and W. Li, *Applied Nonlinear Control*, Prentice-Hall, Englewood Cliffs, NJ, USA, 1991.

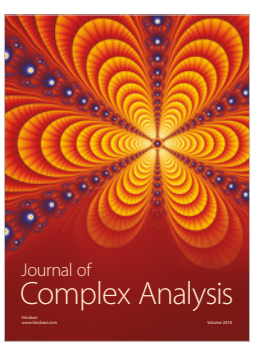
[34] H. Shim, Y. I. Son, and J. H. Seo, "Semi-global observer for multi-output nonlinear systems," *Systems & Control Letters*, vol. 42, no. 3, pp. 233–244, 2001.

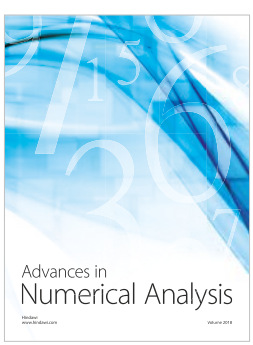


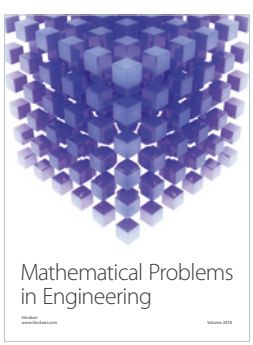


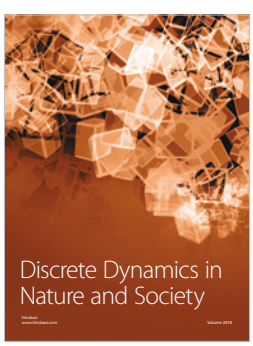


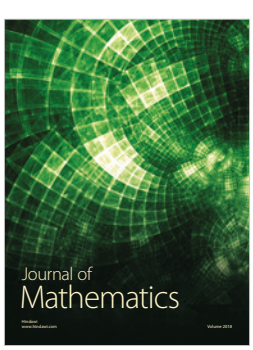


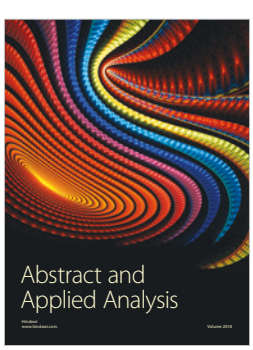


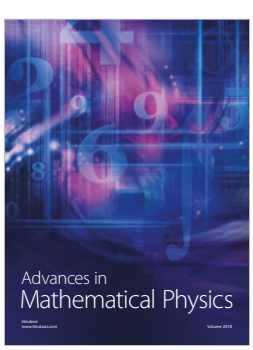












Hindawi

Submit your manuscripts at
www.hindawi.com