Security and Safety, Vol. 1, 2022005 (2022)
https://doi.org/10.1051/sands/2022005
sands.edpsciences.org

Security and Safety

Research Article OPEN ACCESS

Industrial Control

Optimal injection attack strategy for cyber-physical systems: a dynamic feedback approach

Sheng Gao, Hao Zhang*, Zhuping Wang, and Chao Huang

School of Electronics and Information Engineering, Tongji University, Shanghai 201804, China

Received: 30 December 2021 / Revised: 21 February 2022 / Accepted: 14 March 2022 / Published online: 22 July 2022

Abstract This paper investigates the system security problem of cyber-physical systems (CPSs), which is not only more practical but also more significant to deal with than the detecting faults problem. The purpose of this paper is to find an optimal attack strategy that maximizes the output error of the attacked system with low energy consumption. Based on a general model of linear time-invariant systems and a key technical lemma, a new optimal attack strategy for the meticulously designed false data injection attack is constructed. It is worth mentioning that compared with the existing model-based attack strategies, the designed one is more general and the corresponding attack strategy is more easily implemented when system states and external input are inaccessible. Key to overcoming the inaccessible information, a dynamic observer in the form of Luenberger is constructed. Finally, a networked magnetic levitation steel ball movement system is applied to illustrate the effectiveness of the proposed scheme.

Keywords False data injection attack, Dynamic output feedback, Attack strategy design, Cyber-physical systems

Citation Gao S, Zhang H, Wang ZP and et al. Optimal injection attack strategy for cyber-physical systems: a dynamic feedback approach. Security and Safety 2022; **1**: 2022005. https://doi.org/10.1051/sands/2022005

1 Introduction

With the development of computer and communication technology, the network has been rapidly applied to most aspects of society in recent decades. Although the network has brought convenience to people's lives, it is vulnerable to hackers because of its high degree of openness, to name just a few, Bushehr, the only nuclear power plant in Iran, was hacked in 2010 causing all centrifuges to shut down; Colonial Pipeline, the major oil and gas pipeline company in the USA, was hacked in 2021 and forced to shut down all of its pipeline operating systems. Therefore, cyber security is an important part of ensuring national security and social stability. The above systems are classified as the cyber-physical systems[1–3], which integrate computing, networking, and physical processes, whose cyber security has been paid more and more attention by researchers.

Cyber security, which is one of the main issues of informatization, mainly includes cyberattack, attack detection, and security defense. Cyberattack refers to any type of offensive action on a computer equipment, network, or infrastructure from the network layer. There are two commonly used methods for cyberattack, namely, cracking of the system password to steal the information of the attacked system [4–7] and implementing elaborately designed attack strategies to destroy the attacked system [8–15].

[*] Corresponding author (email: zhang_hao@tongji.edu.cn)

Different from the cyberattack on the side of the offensive, attack detection represents the timely discovery of vulnerabilities in the system and alarm from the perspective of the defender. The detection mechanisms for the corresponding attacks have been extensively studied, such as denial-of-service (DoS) attack detection [16], replay attack detection [17], and false data injection (FDI) attack detection [18, 19]. Security defense denotes the security protection of the system from the perspective of the defender. Many researchers have implemented secure control or resilient control strategy under attack to reduce or avoid the damage caused by attackers [20–26]. All of the aforementioned works on cyber security focus on existing classic attack strategies. Unfortunately, the continuous update of attack strategies makes the existing detection mechanisms and defense strategies ineffective. Therefore, this paper mainly designs an attack strategy on the attacker's side. One of the research motivations was to enable defenders to understand the behavior of unknown attackers more deeply, and then design corresponding defense strategies to better protect the system.

To date, two main categories of cyberattacks exist, namely denial-of-service (DoS) attacks [12, 13, 27] and deception attacks, among which deception attacks include replay attacks and injection attacks [10, 28]. DoS attack is destroying the target object, making it unable to serve normal users, resulting in information packet loss or delay, *etc*. Massive research results have been reported on DoS attack strategy design and secure control, see [20–22] and the references therein. The replay attack refers to injecting external inputs without being detected; the attacker hijacks the sensor, observes and records its readings for a period of time, and then repeats these readings when executing the attack [28]. Since the data of replay attack come from a normal system, it is difficult to be detected. Therefore, some detection mechanisms for replay attacks are proposed in [17, 29, 30]. For false data injection attack, the attacker injects the meticulously designed false information to disturb the normal operation of the system. More recently, Chen *et al.* [31] have studied the attack strategy of attackers against CPSs from the vantage point of optimal control. Wu and Jian [32] have also designed a switching data injection attack scheme from the attacker's side. After that, they have further considered the optimal feedback attack problem and the optimal location switching attack problems, respectively [10, 11]. The design of the above attack strategies is based on the assumption that the information of the attacked system is completely known. The fact that a part of the information of the attacked system is inaccessible is a natural extension of the attack strategy design that all information can be accessed. Up to now, when the information of the attacked system is completely unknown, that is, the attacked system is model free for the attacker, there is a neural network learning method to design the attack strategy [33]. However, in most cases, it is a natural fact that the attacker is not completely unaware of the attacked system through long-term information eavesdropping. If the attacked system is regarded as a black box and the attack strategy is directly designed by the learning method, the useful information obtained by eavesdropping will be wasted and the adaptability of the obtained attack strategy will be insufficient. Making good use of this information in the design of attack strategy is the main motivation to promote us to study the problems proposed in this paper.

In this paper, a new attack strategy for cyber-physical systems under the system states and external input inaccessible is proposed. The main contributions of this paper are summarized as follows:

(1) A new data injection attack method is proposed from the perspective of attackers, in which attackers use system output to construct attack strategy in the form of dynamic feedback. The objective function of attacker is defined as the linear quadratic function and the corresponding algebraic Riccati equation is derived by solving the defined objective function.

(2) Since the attacker cannot access the system states and external input information of the attacked system, it is difficult for the attacker to maximize the output error of the attacked system with the least energy consumption. In this paper, a modified Luenberger observer-based method is introduced to solve the aforementioned attack optimization problem.

(3) During the design of the attack strategy, the value of the designed observer is adopted as the dynamic auxiliary virtual states to deal with the difficulty that the unknown parameter matrices of the attack strategy cannot be solved directly.

The rest of this paper is organized as follows. The problem formulation about a class of linear time-invariant system is shown in Section 2. The schemes of dynamic observer and false data injection attack based on dynamic observation and output feedback are described in Section 3. In Section 4, the efficiency of proposed scheme is illustrated by a networked magnetic levitation steel ball movement system example. Finally, this paper is concluded in Section 5.

Notations: $\mathbb{R}^n$ denotes the n-dimensional Euclidean space. Let $M \in \mathbb{R}^{p\times m}$ and $N \in \mathbb{R}^{p\times n}$, $[M, N] \in \mathbb{R}^{p\times(m+n)}$. Let $M \in \mathbb{R}^{m\times p}$ and $N \in \mathbb{R}^{n\times p}$, $[M; N] \in \mathbb{R}^{(m+n)\times p}$. M^T indicates the transposed matrix of matrix M. M^{-1} denotes the inverse matrix of matrix M. $\mathrm{diag}(N, M)$ represents diagonal matrix with diagonal entries N and M. $\mathrm{eig}(M)$ refers to the eigenvalue of matrix M. $\mathrm{Re}(M)$ is defined as the real part of the element of matrix M. $\frac{\partial f}{\partial M}$ stands for the first order partial derivative of f with respect to matrix M. Matrices and vectors are assumed to hold appropriate dimensions if they are not explicitly stated.

2 Problem formulation

Consider a class of linear time-invariant system described by

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + Ed(t), \\ y(t) &= Cx(t) + Du(t) + Fd(t), \end{aligned} \tag{1}$$

where $x \in \mathbb{R}^n$ is the state, $u \in \mathbb{R}^l$ is the control input, $y \in \mathbb{R}^m$ is the measured output, $d(t) \in \mathbb{R}^p$ is the external disturbance, and A, B, C, D, E, and F are known constant matrices with compatible dimensions. External disturbance $d(t)$ is generated by linear autonomous differential equation expressed as

$$\dot{d}(t) = \tilde{A}_d d(t),\ d(0) = d_0, \tag{2}$$

where d_0 is arbitrary initial value.

The tracking error of system (1) can be expressed as

$$e(t) = y(t) - y_r(t), \tag{3}$$

where $y_r(t)$ is the desired output, and $y_r(t)$ is given by

$$\dot{y}_r(t) = \tilde{A}_{yr} y_r(t),\ y_r(0) = y_{r_0}, \tag{4}$$

where y_{r_0} is an arbitrary initial value.

Combining the system state of system (1) and the tracking error (3), the trajectory tracking system can be written as

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) + E_\zeta \zeta(t), \\ y(t) &= Cx(t) + Du(t) + \bar{F}\zeta(t), \\ e(t) &= Cx(t) + Du(t) + F_\zeta \zeta(t), \end{aligned} \tag{5}$$

where

$$\zeta(t) = \begin{bmatrix} y_r(t) \\ d(t) \end{bmatrix}, \begin{bmatrix} E_\zeta \\ \bar{F} \\ F_\zeta \end{bmatrix} = \begin{bmatrix} 0 & E \\ 0 & F \\ -I & F \end{bmatrix},$$

$\zeta(t)$ satisfies

$$\dot{\zeta}(t) = \tilde{A}_\zeta \zeta(t) = \begin{bmatrix} \tilde{A}_{yr} & 0 \\ 0 & \tilde{A}_d \end{bmatrix} \zeta(t),\ \zeta(0) = \zeta_0,$$

where 0 and I are the zero and identity matrix of appropriate dimensions, respectively.

Through the linear quadratic tracker (LQT), the control input is designed as

$$u(t) = K_1 x(t) + K_2 \zeta(t), \tag{6}$$

where K_1 and K_2 are known constant matrices with compatible dimensions.

For system (5), the following assumption is needed.

Assumption 1. The pair (A, B) is stabilizable, $\left([C, \bar{F}], \begin{bmatrix} A & E_\zeta \\ 0 & \tilde{A}_\zeta \end{bmatrix}\right)$ is detectable.

Remark 1. The first part of Assumption 1 is quite standard in the literature to design the attack strategy because it is meaningful for the attackers to destroy stable systems. The latter part of Assumption 1 is necessary for the design of the attack strategy in this paper, when it is undetectable, the attack strategy to achieve the maximum deviation of the system output from the desired output cannot be designed due to the lack of information related to the desired output.

3 Design of optimal data injection attack strategy

3.1 Attack structure

Since the controller transmits the control signal to the actuator through the wireless transmission channel, the attacker achieves the purpose by intercepting the control signal transmitted through the wireless transmission channel and tampering with the signal. The false data injection attack is expressed as

$$\tilde{u}(t) = K_1 x(t) + K_2 \zeta(t) + \Gamma_a u_a(t), \tag{7}$$

where $\tilde{u}(t)$ is the attacked control input, Γ_a is the attack weight matrix with compatible dimension, and $u_a(t) \in \mathbb{R}^q$ is the attack input.

Combining trajectory tracking systems (5) and (7), the attacked system is

$$\begin{aligned} \dot{\tilde{x}}(t) &= (A + BK_1)\tilde{x}(t) + (E_\zeta + BK_2)\zeta(t) + B\Gamma_a u_a(t), \\ \tilde{y}(t) &= (C + DK_1)\tilde{x}(t) + (\bar{F} + DK_2)\zeta(t) + D\Gamma_a u_a(t), \\ \tilde{e}(t) &= (C + DK_1)\tilde{x}(t) + (F_\zeta + DK_2)\zeta(t) + D\Gamma_a u_a(t), \end{aligned} \tag{8}$$

where $\tilde{x}(t)$ and $\tilde{e}(t)$ are the attacked state and unmeasured tracking error, respectively.

The key design of the data injection attack structure is described as

$$\begin{aligned} u_a(t) &= C_a \eta(t), \\ \dot{\eta}(t) &= A_a \eta(t) + B_a \tilde{y}(t), \end{aligned} \tag{9}$$

where A_a, B_a, and C_a are the designed attack matrices with compatible dimensions, $u_a(0)$ is an arbitrarily small initial value and $\eta(t)$ is the designed auxiliary virtual state of the attack input.

The following assumptions are needed to design an attack strategy for the attacker.

Assumption 2. The attacker has complete knowledge of system (5) matrices through eavesdropping the system information for sufficient time.

Assumption 3. In the FDI attack, the attacker has the ability to inject the calculated false data vector $u_a(t)$ into the actuators synchronously with the system input signals.

The purpose of the attacker in this subsection is to use as little energy as possible to make the system tracking error maximum deviate from 0. The objective function can be described as

$$J_1\left(\tilde{e}(t), u_a(t)\right) = \frac{1}{2}\int_{t_0}^{t_f} \left(-\tilde{e}^T(t) Q \tilde{e}(t) + u_a^T(t) R u_a(t)\right) \mathrm{d}t, \tag{10}$$

where t_0 and t_f are the start time and end time of the injection attack, respectively. It is worth mentioning that $u_a^T(t) R u_a(t)$ represents the energy consumption of the attacker. Then, the problem of data injection attack can be expressed as the optimal problem.

Problem 1.

$$\min_{u_a(t)} \quad J_1(\tilde{e}(t), u_a(t))$$

$$\text{s.t.} \begin{cases} \dot{\tilde{x}}(t) = (A + BK_1)\tilde{x}(t) + (E_\zeta + BK_2)\zeta(t) + B\Gamma_a u_a(t), \\ \tilde{e}(t) = (C + DK_1)\tilde{x}(t) + (F_\zeta + DK_2)\zeta(t) + D\Gamma_a u_a(t), \\ \dot{\zeta}(t) = \tilde{A}_\zeta \zeta(t), \\ u_a(t) = C_a \eta(t), \\ \dot{\eta}(t) = A_a \eta(t) + B_a \tilde{y}(t), \\ Q \geq 0, R > 0. \end{cases}$$

Due to inaccessible system states and external input data information from the perspective of the attacker, Problem 1 cannot be solved. Therefore, the dynamic observer is applied in the design of the attack strategy.

3.2 Design of dynamic observer

Note that system state $\tilde{x}(t)$, external disturbance $d(t)$, and desired output $y_r(t)$ are unknown to the attacker. Thus, the attacker can use the modified Luenberger observer to observe state $x(t)$ and external input $\zeta(t)$, the observer is designed as

$$\dot{\xi}(t) = \bar{A}\xi(t) + \bar{B}\hat{\tilde{u}}(t) + L(\tilde{y}(t) - \bar{C}\xi(t) - D\hat{\tilde{u}}(t)), \tag{11}$$

where $\xi(t)$ is the estimation of $[x(t), \zeta(t)]^T$, $\hat{\tilde{u}}(t)$ is the estimated control input based on the observation of $[x(t), \zeta(t)]^T$, which satisfies $\hat{\tilde{u}}(t) = [K_1, K_2]\xi(t) + \Gamma_a u_a(t)$, L is the observation matrix, and $\bar{A} = \begin{bmatrix} A & E_\zeta \\ 0 & \tilde{A}_\zeta \end{bmatrix}$, $\bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}$, and $\bar{C} = [C, \bar{F}]$.

Lemma 1. Under Assumptions 1, for the attacked system (8) and the observer (11), if L satisfies the condition $\mathrm{Re}(\mathrm{eig}(\bar{A} - L\bar{C} + (\bar{B} - LD)[K_1, K_2])) < 0$, then $\lim_{t\to\infty} e_{x\xi}(t) = 0$, where $e_{x\xi}(t) = [x(t), \zeta(t)]^T - \xi(t)$ denotes the observation error.

Proof. Combined with $\tilde{u}(t)$, $\hat{\tilde{u}}(t)$, the attacked system (8) and the observer (11), the derivative of the observation error $e_{x\xi}(t)$ can be expressed as

$$\begin{aligned}
\dot{e}_{x\xi}(t) &= \begin{bmatrix} \dot{\tilde{x}}(t) \\ \dot{\zeta}(t) \end{bmatrix} - \dot{\xi}(t) \\
&= \bar{A}\begin{bmatrix} \tilde{x}(t) \\ \zeta(t) \end{bmatrix} + \bar{B}\tilde{u}(t) - \left[\bar{A}\xi(t) + \bar{B}\hat{\tilde{u}}(t) + L\left(\tilde{y}(t) - \bar{C}\xi(t) - D\hat{\tilde{u}}(t)\right)\right], \\
&= \bar{A}\begin{bmatrix} \tilde{x}(t) \\ \zeta(t) \end{bmatrix} + \bar{B}\left([K_1, K_2]\begin{bmatrix} \tilde{x}(t) \\ \zeta(t) \end{bmatrix} + \Gamma_a u_a(t)\right) - \Bigg[\bar{A}\xi(t) + \bar{B}\left([K_1, K_2]\,\xi(t) + \Gamma_a u_a(t)\right) \\
&\quad + L\Bigg(\left[(C + DK_1), (\bar{F} + DK_2)\right]\begin{bmatrix} \tilde{x}(t) \\ \zeta(t) \end{bmatrix} + D\Gamma_a u_a(t) - \bar{C}\xi(t) - D\left([K_1, K_2]\xi(t) + \Gamma_a u_a(t)\right)\Bigg)\Bigg], \\
&= \left(\bar{A} - L\bar{C} + (\bar{B} - LD)[K_1, K_2]\right)\left(\begin{bmatrix} \tilde{x}(t) \\ \zeta(t) \end{bmatrix} - \xi(t)\right), \\
&= \left(\bar{A} - L\bar{C} + (\bar{B} - LD)[K_1, K_2]\right)e_{x\xi}(t),
\end{aligned} \tag{12}$$

thus, through the theory of observer design, when $\mathrm{Re}\left(\mathrm{eig}\left(\bar{A} - L\bar{C} + (\bar{B} - LD)[K_1, K_2]\right)\right) < 0$ is satisfied, $\lim_{t\to\infty} e_{x\xi}(t) = 0$, which indicates that when $t \to \infty$, the estimation $\xi(t)$ is equal to $[x(t), \zeta(t)]^T$.

This is end of proof □

It is worth pointing out that the designed auxiliary virtual state $\eta(t)$ is determined by the attacker. When observation $\xi(t)$ is selected by the attacker as the designed auxiliary virtual state $\eta(t)$, Problem 1 can be transformed into Problem 2.

Problem 2.

$$\begin{aligned}
&\min_{u_a(t)} \quad J_1(\hat{\tilde{e}}(t), u_a(t)) \\
&\text{s.t.} \quad \begin{cases}
\dot{\xi}(t) = \bar{A}\xi(t) + \bar{B}\hat{\tilde{u}}(t) + L(\tilde{y}(t) - \bar{C}\xi(t) - D\hat{\tilde{u}}(t)), \\
\hat{\tilde{e}}(t) = [(C + DK_1), (F_\zeta + DK_2)]\xi(t) + D\Gamma_a u_a(t), \\
\hat{\tilde{u}}(t) = [K_1, K_2]\xi(t) + \Gamma_a u_a(t), \\
u_a(t) = C_a\eta(t), \\
\dot{\eta}(t) = A_a\eta(t) + B_a\tilde{y}(t), \\
\eta(t) = \xi(t), \\
Q \geq 0, R > 0.
\end{cases}
\end{aligned}$$

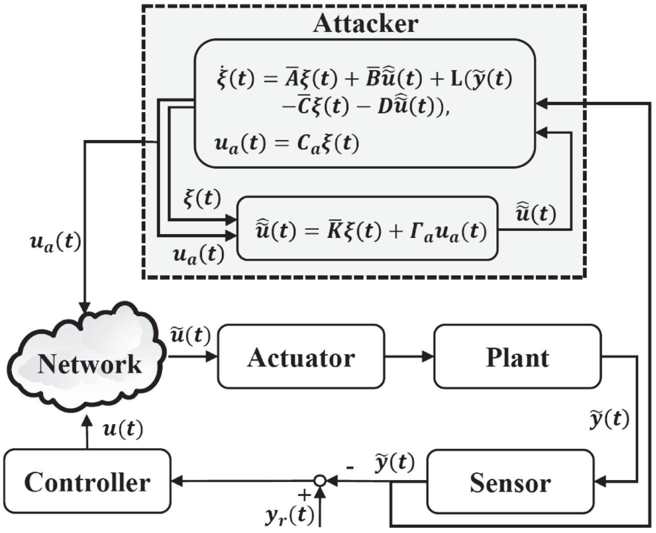
Attacker
$\dot{\xi}(t) = \bar{A}\xi(t) + \bar{B}\hat{\tilde{u}}(t) + L(\tilde{y}(t)$
$-\bar{C}\xi(t) - D\hat{\tilde{u}}(t)),$
$u_a(t) = C_a\xi(t)$
$\xi(t)$
$\hat{\tilde{u}}(t) = \bar{K}\xi(t) + \Gamma_a u_a(t)$
$\hat{\tilde{u}}(t)$
$u_a(t)$
$u_a(t)$
Network
$\tilde{u}(t)$
Actuator
Plant
$\tilde{y}(t)$
$u(t)$
Controller
-
$\tilde{y}(t)$
Sensor
+
$y_r(t)$

Figure 1. Block diagram of the attacked system

The block diagram of the attacked system is shown in Figure 1. As can be seen from Figure 1, the attacker first obtains the system output $\tilde{y}(t)$ by eavesdropping, which is transmitted from the plant to the controller using the sensor. Then, system output $\tilde{y}(t)$ and the estimated value of the designed observer are applied to construct (9). Next, optimal attack input $u_a(t)$ can be obtained by solving Problem 2. Finally, optimal attack input $u_a(t)$ is injected into control input $u(t)$ wirelessly transmitted from the controller to the actuator so that the control input obtained by the actuator is tampered with $\tilde{u}(t)$ to complete the attack.

3.3 Main results

Before presenting the main result, the key lemma is first introduced.

Lemma 2 ([34, 35]). The optimal problem is expressed as

$$\begin{aligned} \min_{u(t)} \quad & J_2(x(t), u(t)) = \frac{1}{2}\int_{t_0}^{t_f} \left(x^T(t)Qx(t) + u^T(t)Ru(t)\right) \mathrm{d}t \\ \text{s.t.} \quad & \begin{cases} \dot{x}(t) = Ax(t) + Bu(t), \\ Q \geq 0, R > 0. \end{cases} \end{aligned}$$

If requirement $Q \geq 0$ is not satisfied, a necessary and sufficient condition to provide a unique solution to the affine-quadratic continuous-time optimal problem is

$$R + B^T PB > 0,$$

where P is the solution of the following Algebraic Riccati Equation

$$PA + A^T P - P\left(R + B^T PB\right)^{-1} P + Q = 0.$$

Theorem 1. Under Assumptions 1–3, if $\left(R - \Gamma_a^T D^T QD\Gamma_a\right) > 0$ holds and the observation $\xi(t)$ is selected by the attacker as the designed auxiliary virtual state $\eta(t)$, the matrices of the optimal attack strategy designed as (9) can be obtained by solving Problem 2, which are expressed as

$$\begin{aligned} & A_a = \bar{A} + \bar{B}\bar{K} - L\bar{C} - LD\bar{K} + (\bar{B} - LD)\Gamma_a\left(R - \Gamma_a^T D^T QD\Gamma_a\right)^{-1}\left(\Gamma_a^T D^T Q\bar{C}_e - \Gamma_a^T D^T B_a^T P\right), \\ & B_a = L, \\ & C_a = \left(R - \Gamma_a^T D^T QD\Gamma_a\right)^{-1}\left(\Gamma_a^T D^T Q\bar{C}_e - \Gamma_a^T D^T B_a^T P\right) \end{aligned} \tag{13}$$

where P satisfies the following equation

$$P\Xi + \Xi^T P - P\Psi P - \Theta = 0, \tag{14}$$

and

$$\begin{aligned}
&\Xi = \bar{A} + \bar{B}\bar{K} - L(\bar{C} - \tilde{C}) + \bar{B}\Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T Q \bar{C}_e,\\
&\Psi = \bar{B}\Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T B_a^T - B_a D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T B_a^T + B_a D \Gamma_a\\
&\qquad \times \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T \bar{B}^T,\\
&\Theta = \bar{C}_e^T Q \bar{C}_e + \bar{C}_e Q D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T Q \bar{C}_e,\\
&\bar{C}_e = \tilde{C} + D\bar{K},\ \tilde{C} = [C, F_\zeta],\ \bar{K} = [K_1, K_2].
\end{aligned}$$

Proof. If the attacker utilizes observation $\xi(t)$ as designed auxiliary virtual state $\eta(t)$, then attacked control input (7) based on the observation of $[x(t), \zeta(t)]^T$ can be rewritten as

$$\begin{aligned}
\hat{\tilde{u}}(t) &= [K_1, K_2]\eta(t) + \Gamma_a u_a(t),\\
&\triangleq \bar{K}\eta(t) + \Gamma_a u_a(t),
\end{aligned} \tag{15}$$

where $\bar{K}$ is described in Theorem 1.

Combining (9), (11) and (15), one has

$$\begin{aligned}
\dot{\eta}(t) &= \bar{A}\eta(t) + \bar{B}\bar{K}\eta(t) + \bar{B}\Gamma_a u_a(t) + L(\tilde{y}(t) - \bar{C}\eta(t) - D\bar{K}\eta(t) - D\Gamma_a u_a(t)),\\
&= (\bar{A} + \bar{B}\bar{K} - L\bar{C} - LD\bar{K} + (\bar{B} - LD)\Gamma_a C_a)\eta(t) + L\tilde{y}(t),
\end{aligned} \tag{16}$$

thus, $A_a = \bar{A} + \bar{B}\bar{K} - L\bar{C} - LD\bar{K} + (\bar{B} - LD)\Gamma_a C_a$ and $B_a = L$.

Inserting (15) into the attacked tracking error $\tilde{e}(t)$ based on the observation of $[x(t), \zeta(t)]^T$, one has

$$\hat{\tilde{e}}(t) = [(C + DK_1), (F_\zeta + DK_2)]\eta(t) + D\Gamma_a u_a(t) = \bar{C}_e\eta(t) + D\Gamma_a u_a(t), \tag{17}$$

therefore, the integrated term of the objective function (10) can be reorganized as

$$\begin{aligned}
&- \hat{\tilde{e}}^T(t) Q \hat{\tilde{e}}(t) + u_a^T(t) R u_a(t),\\
&= -\left(\bar{C}_e\eta(t) + D\Gamma_a u_a(t)\right)^T Q \left(\bar{C}_e\eta(t) + D\Gamma_a u_a(t)\right) + u_a^T(t) R u_a(t),\\
&= -\eta^T(t)\bar{C}_e^T Q \bar{C}_e \eta(t) - \eta^T(t)\bar{C}_e^T Q D \Gamma_a u_a(t) - u_a^T(t)\Gamma_a^T D^T Q \bar{C}_e \eta(t) + u_a^T(t)\left(R - \Gamma_a^T D^T Q D \Gamma_a\right) u_a(t),
\end{aligned} \tag{18}$$

then, the Hamilton function is defined as

$$\begin{aligned}
\mathrm{H}\left(\eta(t), u_a(t), \lambda(t), t\right) =& \frac{1}{2}\left(-\eta^T(t)\bar{C}_e^T Q \bar{C}_e \eta(t) - \eta^T(t)\bar{C}_e^T Q D \Gamma_a u_a(t) - u_a^T(t)\Gamma_a^T D^T Q \bar{C}_e \eta(t)\right.\\
&\left.+ u_a^T(t)\left(R - \Gamma_a^T D^T Q D \Gamma_a\right) u_a(t)\right) + \lambda^T(t)\left(A_a\eta(t) + B_a\bar{C}_e\eta(t) + B_a D \Gamma_a u_a(t)\right),
\end{aligned} \tag{19}$$

where $\lambda(t)$ is the co-state vector.

Through the optimal theory [35], $\frac{\partial \mathrm{H}}{\partial u_a(t)} = 0$ is applied,

$$\frac{\partial \mathrm{H}}{\partial u_a(t)} = -\Gamma_a^T D^T Q \bar{C}_e \eta(t) + \left(R - \Gamma_a^T D^T Q D \Gamma_a\right) u_a(t) + \Gamma_a^T D^T B_a^T \lambda(t) = 0, \tag{20}$$

the optimal attack input is obtained as

$$u_a^*(t) = \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1}(\Gamma_a^T D^T Q \bar{C}_e \eta(t) - \Gamma_a^T D^T B_a^T \lambda(t)\big), \tag{21}$$

combined with the co-state equation,

$$\begin{aligned}\dot{\lambda}(t) = -\frac{\partial \mathrm{H}}{\partial \eta(t)} &= \bar{C}_e^T Q \bar{C}_e \eta(t) + \bar{C}_e^T Q D \Gamma_a u_a(t) - (A_a + B_a \bar{C}_e)^T \lambda(t), \\ &= \bar{C}_e^T Q \bar{C}_e \eta(t) + \bar{C}_e^T Q D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} (\Gamma_a^T D^T Q \bar{C}_e \eta(t) - \Gamma_a^T D^T B_a^T \lambda(t)) \\ &\quad - \left(A_a + B_a \bar{C}_e\right)^T \lambda(t), \\ &= \left[\bar{C}_e^T Q \bar{C}_e + \bar{C}_e Q D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T Q \bar{C}_e\right] \eta(t) - \left[\left(A_a + B_a \bar{C}_e\right)^T \right. \\ &\quad \left. + \bar{C}_e^T Q D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T B_a^T\right] \lambda(t),\end{aligned} \tag{22}$$

letting $\lambda(t) = P\eta(t)$, (21) and (22) can be rewritten as

$$u_a^*(t) = \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \left(\Gamma_a^T D^T Q \bar{C}_e - \Gamma_a^T D^T B_a^T P\right) \eta(t) = C_a \eta(t), \tag{23}$$

thus, C_a is obtained, and

$$\begin{aligned}\dot{\lambda}(t) &= P\dot{\eta}(t) \\ &= P\left(\left(A_a + B_a \bar{C}_e\right) \eta(t) + B_a D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \left(\Gamma_a^T D^T Q \bar{C}_e - \Gamma_a^T D^T B_a^T P\right) \eta(t)\right),\end{aligned} \tag{24}$$

Since (22) and (24) are equal, the preliminary algebraic Riccati equation can be described as

$$\begin{aligned}&P\left(\left(A_a + B_a \bar{C}_e\right) + B_a D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \left(\Gamma_a^T D^T Q \bar{C}_e - \Gamma_a^T D^T B_a^T P\right)\right) = \left[\bar{C}_e^T Q \bar{C}_e + \bar{C}_e Q D \right. \\ &\left. \times \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T Q \bar{C}_e\right] - \left[\left(A_a + B_a \bar{C}_e\right)^T + \bar{C}_e^T Q D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T B_a^T\right] P,\end{aligned} \tag{25}$$

by means of Lemma 2, the optimal solution for Problem 2 is unique if and only if $\left(R - \Gamma_a^T D^T Q D \Gamma_a\right) > 0$.

Since A_a contains C_a, C_a contains P, and (25) contains A_a, in order to avoid the unknown matrix when solving in (25), combining (16), (23), and (25), one can obtain

$$\begin{aligned}&P\left[\bar{A} + \bar{B}\bar{K} - L\bar{C} - LD\bar{K} + \left(\bar{B} - LD\Gamma_a\right) \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \left(\Gamma_a^T D^T Q \bar{C}_e - \Gamma_a^T D^T B_a^T P\right) + B_a \bar{C}_e \right. \\ &\left. + B_a D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \left(\Gamma_a^T D^T Q \bar{C}_e - \Gamma_a^T D^T B_a^T P\right)\right] + \left[\bar{A} + \bar{B}\bar{K} - L\bar{C} - LD\bar{K} + \left(\bar{B} - L \right.\right. \\ &\left. \times D\Gamma_a\right) \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \left(\Gamma_a^T D^T Q \bar{C}_e - \Gamma_a^T D^T B_a^T P\right) + B_a \bar{C}_e + B_a D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \\ &\left. \times \left(\Gamma_a^T D^T Q \bar{C}_e - \Gamma_a^T D^T B_a^T P\right)\right]^T P - P B_a D \Gamma_a (R - \Gamma_a^T D^T Q D \Gamma_a)^{-1} \Gamma_a^T D^T B_a^T P - \bar{C}_e^T Q \bar{C}_e + \bar{C}_e Q \\ &\times D \Gamma_a \left(R - \Gamma_a^T D^T Q D \Gamma_a\right)^{-1} \Gamma_a^T D^T Q \bar{C}_e = 0,\end{aligned} \tag{26}$$

then, $B_a = L$ and $\bar{C}_e = [C, F_\zeta] + D\bar{K}$ are used to simplify (26) to obtain (14).

This is end of proof. □

The application of Theorem 1 is transformed into the false data injection attack algorithm based on dynamic observation feedback, as shown in Algorithm 1.

Remark 2. In Algorithm 1, the Euler forward discretization method is adopted in the practical application of attack strategy, and other discretization methods can also be applied, such as trapezoidal rule, Heun method, Runge Kutta method, *etc.*

Algorithm 1 . The false data injection attack algorithm based on dynamic observation feedback.

```
Initialize: The system matrices $A$, $B$, $C$, $D$, $E_\zeta$, $F_\zeta$, $\tilde{A}_\zeta$, $K_1$, and $K_2$;
            Set sampling time $\tau$, the start time and end time of the injection attack $t_0$ and $t_f$,
            suitable initial observation $\eta(0)$, and suitable weighting matrices $Q$ and $R$, satisfying
            $Q \geq 0$ and $R > 0$.
Step 1. Calculate the matrices of the observer, $\bar{A}, \bar{B}, \bar{C}$;
        Select suitable observation matrix $L$, satisfying $\mathrm{Re}(\mathrm{eig}(\bar{A} - L\bar{C} + (\bar{B} - LD)[K_1, K_2])) < 0$;
        Set weight attack matrix $\Gamma_a$, satisfying $(R - \Gamma_a^T D^T Q D \Gamma_a) > 0$;
        Calculate matrices $\bar{C}_e$, $\bar{K}$, $\Xi$, $\Psi$, $\Theta$ and solve equation (14) to obtain $P$;
        Calculate matrices of the attack strategy $A_a$, $B_a$, and $C_a$.
while $t \leq t_f$ do
    Step 2. Update $\eta(t)$, $\tilde{y}(t)$ and $\hat{\tilde{u}}(t+\tau)$;
            Calculate observation $\eta(t+\tau)$ as calculate $\eta(t+\tau) \longleftarrow (A_a\tau + I)\eta(t) + B_a\tau\tilde{y}(t)$ or
            $\eta(t+\tau) \longleftarrow (\tau\bar{A} + I)\eta(t) + \tau\bar{B}\hat{\tilde{u}}(t) + L\tau(\tilde{y}(t) - \bar{C}\xi(t) - D\hat{\tilde{u}}(t))$.
    Step 3. Calculate optimal attack input $u_a^*(t+\tau)$ as $u_a^*(t+\tau) \longleftarrow C_a\eta(t+\tau)$,
            and implement injection attack $\hat{\tilde{u}}(t+\tau) \longleftarrow [K_1, K_2]\eta(t+\tau) + \Gamma_a u_a(t+\tau)$.
end while
```

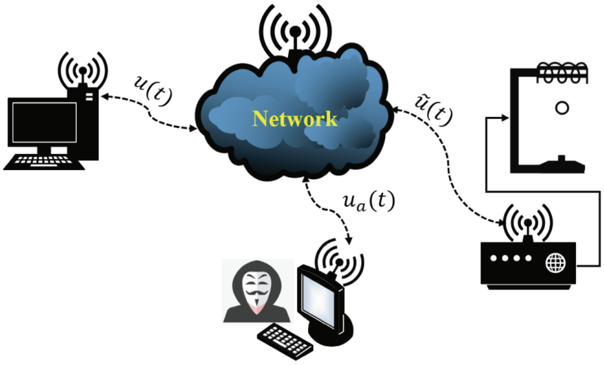

Figure 2. The schematic diagram of the networked magnetic levitation steel ball movement system under attack

4 Simulation example

A networked magnetic levitation steel ball movement system [36] is applied to illustrate the effectiveness of the designed attack strategy. The schematic diagram of the networked magnetic levitation steel ball movement system which is attacked is shown in Figures 2 and 3, where the networked magnetic levitation steel ball motion system can be described as

$$\dot{x}(t) = \begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 9 & 0 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \end{bmatrix} u(t) + \begin{bmatrix} 0.01 \\ 0.015 \end{bmatrix} d(t),$$

$$u(t) = K_1 \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + K_2 \begin{bmatrix} y_r(t) \\ d(t) \end{bmatrix},$$

$$y(t) = \begin{bmatrix} 0 & 1 \end{bmatrix} \begin{bmatrix} x_1(t) \\ x_2(t) \end{bmatrix} + 0.01u(t) + 0.002d(t),$$

where the physical meaning and unit represented by each variable are shown in Table 1, external disturbance input $d(t)$, desired system output $y_r(t)$, and tracking error $e(t)$ can be expressed as

$$\dot{d}(t) = -0.2d(t), \ d(0) = 0.1,$$

$$\dot{y}_r(t) = -0.1y_r(t), \ y_r(0) = 1,$$

$$e(t) = y(t) - y_r(t).$$

The initial system state $x(0) = [-1; 2]$, the initial control input $u(0) = 0.2$, and the control feedback gain $K_1 = [-11.13, -2.92]$, $K_2 = [1, 0]$. The simulation terminal time $t_f = 50$ s, the sampling

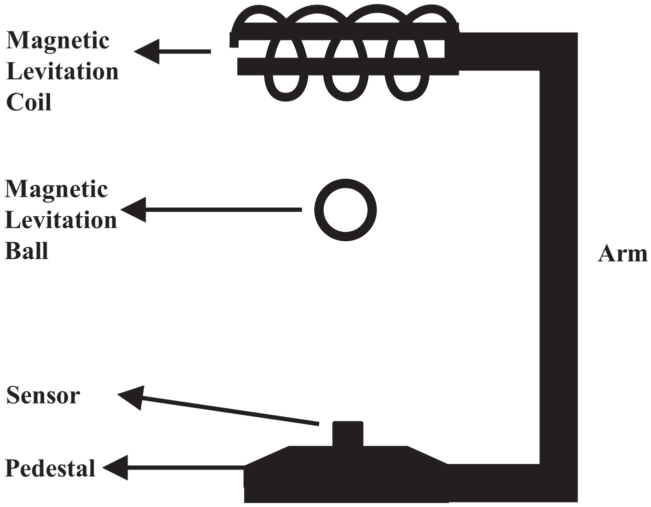

Figure 3. The structure diagram of the networked magnetic levitation steel ball movement system

Table 1. Specifications of the networked magnetic levitation steel ball movement system

Symbol	Description	Value/Unit
$x_1(t)$	Position of magnetic levitation ball at time t	–/mm
$x_2(t)$	Velocity of magnetic levitation ball at time t	–/mm/s
$u(t)$	Voltage across the suspension winding coil at time t	–/V
$y(t)$	Actual output of the system at time t	–
$y_r(t)$	Desired system output at time t	–
$d(t)$	External disturbance input at time t	–

time $\tau = 0.12$, the suitable observation matrix $L = \begin{bmatrix} -14.2446 \\ -0.8097 \\ -34.5498 \\ 163.0878 \end{bmatrix}$, $\mathrm{eig}(\bar{A} - L\bar{C} + (\bar{B} - LD)[K_1, K_2]) = \begin{bmatrix} -1.1071 \\ -0.9935 + 0.0999\mathrm{i} \\ -0.9935 - 0.0999\mathrm{i} \\ -0.9060 \end{bmatrix}$ satisfies $\mathrm{Re}(\mathrm{eig}(\bar{A} - L\bar{C} + (\bar{B} - LD)[K_1, K_2])) < 0$, weight attack matrix $\Gamma_a = 10$, weighting matrices of objective function $Q = 1$ and $R = 1$, satisfies $(R - \Gamma_a^T D^T Q D \Gamma_a) = 0.99 > 0$, and initial attack input $u_a(0) = 0.5$, and simulation results are shown in Figures 4–9.

The designed attack strategy matrix is obtained as follows,

$$A_a = \begin{bmatrix} -6.2445 & 14.5448 & 90.4612 & 18.8442 \\ -35.1926 & -4.1429 & 640.1980 & 133.1055 \\ -15.1458 & 32.8524 & 219.3106 & 45.6817 \\ 71.4938 & -155.0755 & -1035.6988 & -215.8346 \end{bmatrix}, B_a = \begin{bmatrix} -14.2446 \\ -0.8097 \\ -34.5498 \\ 163.0878 \end{bmatrix},$$
$$C_a = \begin{bmatrix} -3.2708 & -0.1993 & 63.4056 & 13.2020 \end{bmatrix}.$$

It is worth noting that the output of the networked magnetic levitation steel ball movement system can be eavesdropped by the attacker, but the system states, desired output, and external disturbance input cannot be obtained for the attacker.

The results in Figures 4, 5 and 8 show the comparison of system states, output, and output error under healthy and attacked conditions. It can be seen that the damage effect of the attack

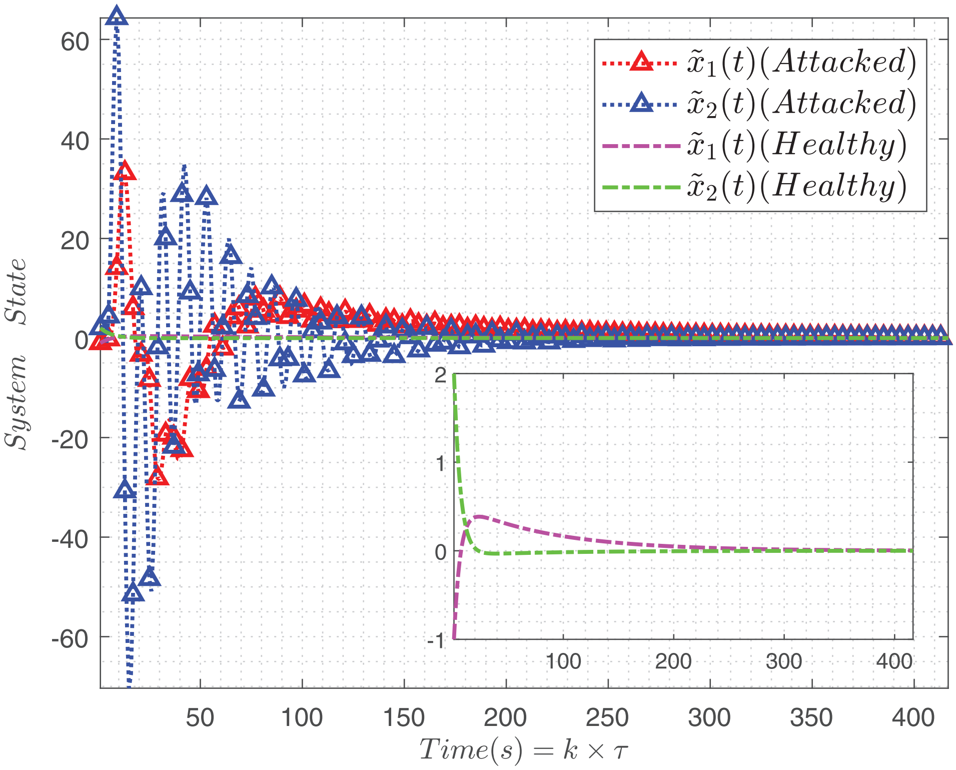

Figure 4. The networked magnetic levitation steel ball movement system states under healthy and attacked conditions

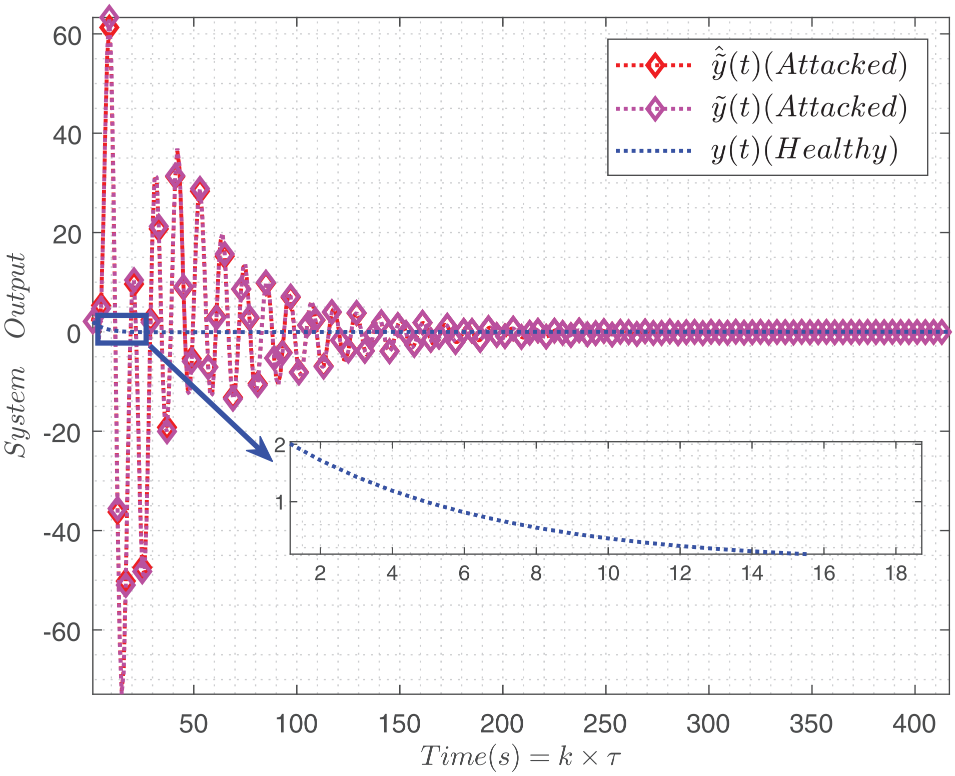

Figure 5. The health output, real output under the attack condition and observation-based output under the attack condition of the networked magnetic levitation steel ball movement system

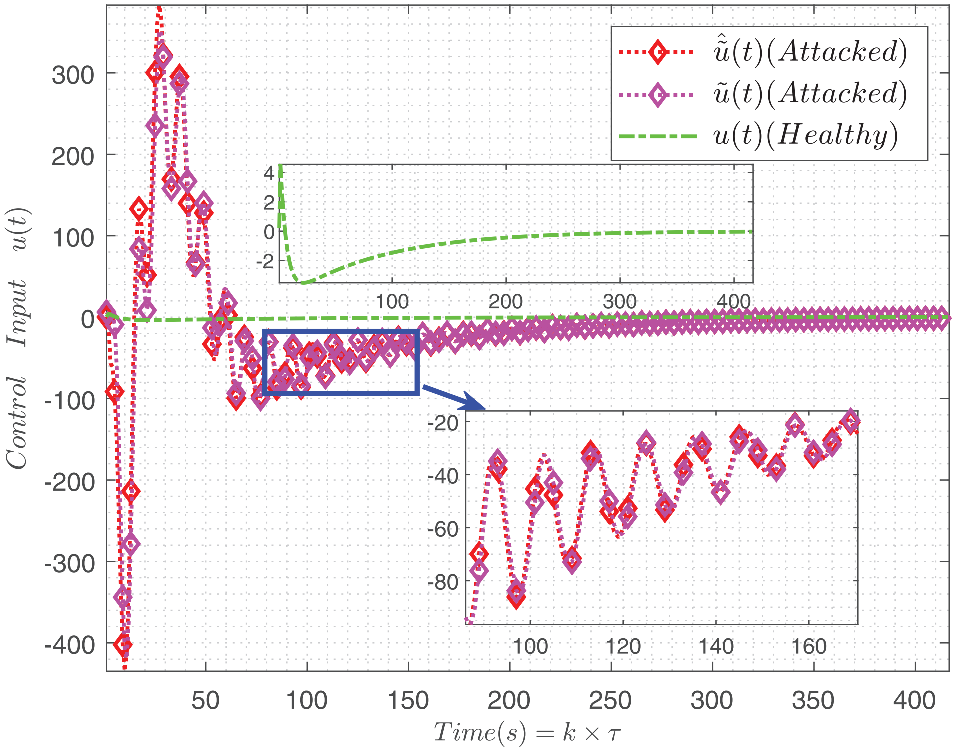

Figure 6. The health control input, real control input under the attack condition and observation-based control input under the attack condition of the networked magnetic levitation steel ball movement system

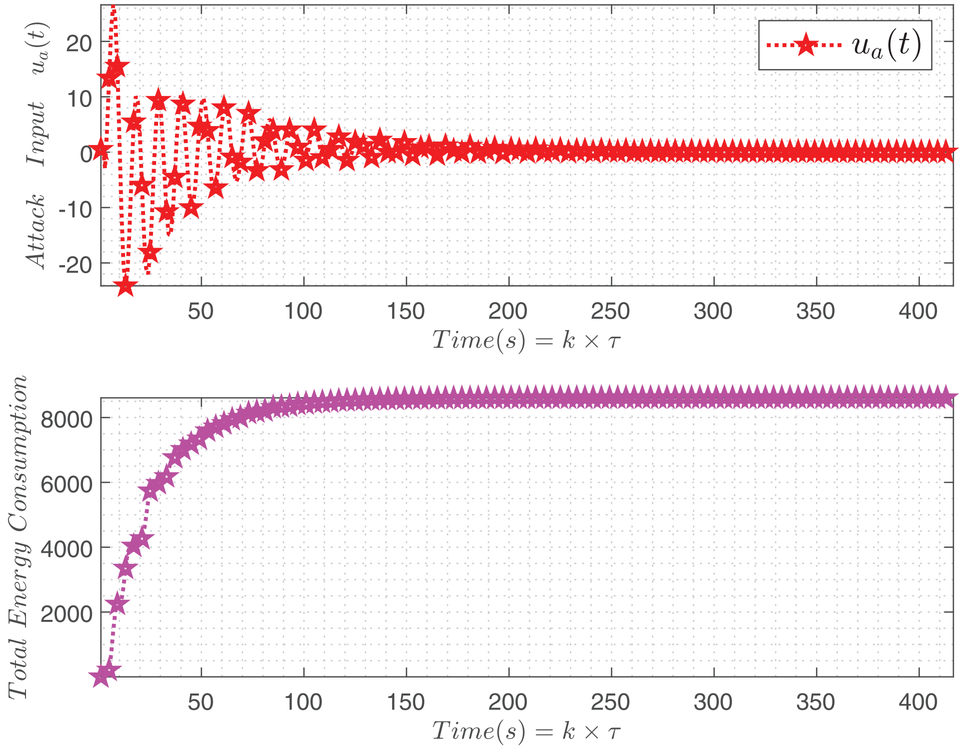

Figure 7. The designed optimal attack output curve and total energy consumption of the attacker

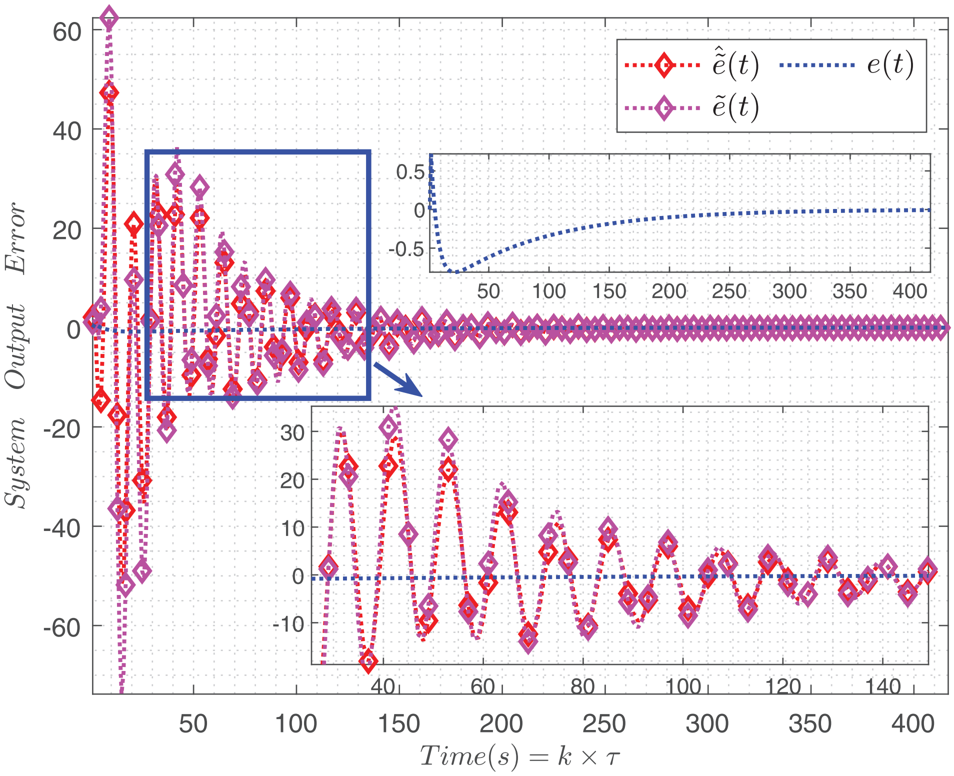

Figure 8. The health output error, real output error under the attack condition and observation-based output error under the attack condition of the networked magnetic levitation steel ball movement system

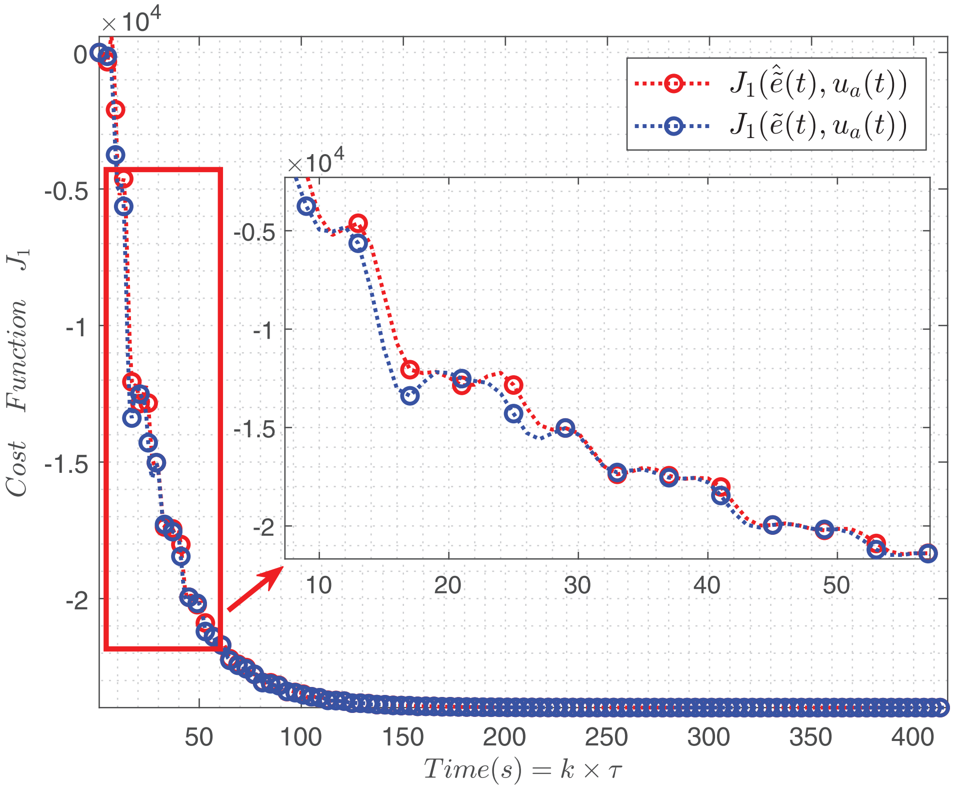

Figure 9. The cost function value calculated by real output error and the observation-based output error under the attack condition

Table 2. Comparison of different attack strategies

Attack strategies	Whether the system matrices are required	Whether the attack strategy can be implemented without obtaining the system state
Strategies in ([32], 2016)	Yes	No
Strategies in ([10], 2018)	Yes	No
Strategies in ([11], 2021)	Yes	No
This study	Yes	Yes

is large. In addition, in Figures 5 and 8, the error between the real output and the output based on observation is small enough; the real output error and output error based on observation indicates that the observation error of the designed observer is small. The result in Figure 7 shows the designed attack strategy and the total energy consumption of the attacker, the total energy consumption of the attacker converges to the optimal value 8607.9, and the result in Figure 9 that the variation form of the cost function based on the real output error and the observed output error is basically the same or even better, and converges to the same optimal value, $J^* = -23992$.

It can be known from Table 2 that the attack strategy designed in this paper relaxes the requirements for obtaining the state information of the attacked system under the assumption that the system matrix information is known. When the system state and external input of the system cannot be stolen by the attacker, the attack strategy involved in Wu *et al.* [10, 11, 32] cannot be adopted by the attacker. Since the attack strategy in this paper is based on the integrated strategy of dynamic observation and output feedback, it can effectively solve the problem that the part of the attacked system information can be known.

5 Conclusion

This paper has proposed a new optimal attack strategy based on dynamic observation and output feedback to achieve the attack purpose that maximizes the output error of the attacked system under the minimum energy consumption of the attacker. The proposed attack strategy does not require the full state information and external input information of the attacked system. Future work includes the design of attack strategy using dynamic output feedback under non-observation, and the design of attack strategy when there is an unknown time delay in the attack.

Conflict of Interest

The authors declare that they have no conflict of interest.

Data Availability

The original data are available from corresponding authors upon reasonable request.

Authors' Contributions

Sheng Gao wrote and constructed this paper. Hao Zhang mainly surveyed the related work and jointly wrote this paper. Zhuping Wang discussed the recent development, corrects typos in the paper and jointly wrote this paper. Chao Huang carried out the theoretical derivation inspection and simulation experiment assistance.

Acknowledgements

We would like to thank all editors and reviewers who help us improve the paper.

Funding

This work is supported by National Natural Science Foundation of China (61922063), Shanghai International Science and Technology Cooperation Project (18510711100), Shanghai Shuguang Project (18sg18), Shanghai Natural Science Foundation (19zr1461400), Shanghai Sailing Program under grant (20YF1452900), Shanghai Municipal Science and Technology Major Project (2021SHZDZX0100), Shanghai Hong Kong Macao Taiwan Science and Technology Cooperation Project (21550760900) and Fundamental Research Funds for the Central Universities.

References

[1] Wolf W. Cyber-physical systems. Computer 2009; **42**: 88–9.

[2] Humayed A, Lin J and Li F et al. Cyber-physical systems security: a survey. IEEE Internet Things J 2017; **4**: 1802–31.

[3] Ashibani Y and Mahmoud QH. Cyber-physical systems security: analysis, challenges and solutions. Comput Secur 2017; **68**: 81–97.

[4] Weir M, Aggarwal S and Medeiros BD et al. Password cracking using probabilistic context-free grammars. In: 2009 30th IEEE Symposium on Security and Privacy, 17–20 May 2009, Oakland, CA, USA, 2009, 391–405.

[5] Houshmand S, Aggarwal S and Flood R. Next gen PCFG password cracking. IEEE Trans Inf Forensics Secur 2015; **10**: 1776–91.

[6] Ji S, Yang S and Hu X et al. Zero-sum password cracking game: a large-scale empirical study on the crackability, correlation, and security of passwords. IEEE Trans Dependable Secure Comput 2017; **14**: 550–64.

[7] Shayan M, Bhattacharjee S and Orozaliev A et al. Thwarting Bio-IP theft through dummy-valve-based obfuscation. IEEE Trans Inf Forensics Secur 2021; **16**: 2076–89.

[8] Kosut O, Jia L and Thomas RJ et al. Limiting false data attacks on power system state estimation. In: 2010 44th Annual Conference on Information Sciences and Systems (CISS), 17–19 March 2010, Princeton, NJ, 2010, 1–6.

[9] Xie L, Mo Y and Sinopoli B. Integrity data attacks in power market operations. IEEE Trans Smart Grid 2011; **2**: 659–66.

[10] Wu G, Jian S and Jie C. Optimal data injection attacks in cyber-physical systems. IEEE Trans Cybern 2018; **48**: 3302–12.

[11] Wu G, Wang G and Sun J et al. Optimal switching attacks and countermeasures in cyber-physical systems. IEEE Trans Syst Man Cybern Syst 2021; **51**: 4825–35.

[12] Imer O, Yüksel S and Başar T. Optimal control of LTI systems over unreliable communication links. Automatica 2006; **42**: 1429–39.

[13] Befekadu GK, Gupta V and Antsaklis PJ. Risk-sensitive control under Markov modulated denial-of-service (DoS) attack strategies. IEEE Trans Automat Contr 2015; **60**: 3299–304.

[14] Koning W. Infinite horizon optimal control of linear discrete time systems with stochastic parameters. Automatica 1982; **18**: 443–53.

[15] Katayama T. On the matrix Riccati equation for linear systems with random gain. IEEE Trans Automat Contr 1976; **21**: 770–1.

[16] Jiang X, Yang J and Jin G et al. RED-FT: A scalable random early detection scheme with flow trust against DoS attacks. IEEE Commun Lett 2013; **17**: 1032–5.

[17] Guo H, Pang Z-H and Sun J et al. An output-coding-based detection scheme against replay attacks in cyber-physical systems. IEEE Trans Circuits Syst II Express Br 2021; **68**(10): 3306–10.

[18] Mo Y, Chabukswar R and Sinopoli B. Detecting integrity attacks on scada systems. IEEE Trans Control Syst Technol 2014; **22**: 1396–1407.

[19] Mo Y, Weerakkody S and Sinopoli B. Physical authentication of control systems: Designing watermarked control inputs to detect counterfeit sensor outputs. IEEE Control Syst Mag 2015; **35**: 93–109.

[20] Sinopoli B, Schenato L and Franceschetti M et al. Optimal control with unreliable communication: the TCP case. In: Proceedings of the 2005 American Control Conference, 8–10 June 2005, Portland, OR, USA, **Vol. 5**, 2005, 3354–59.

[21] Zhang H, Cheng P and Shi L et al. Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans Automat Contr 2015; **60**: 3023–8.

[22] Ding K, Li Y and Quevedo DE et al. A multi-channel transmission schedule for remote state estimation under DoS attacks. Automatica 2017; **78**: 194–201.

[23] Xu Y, Zhou J and Rao H et al. Reset moving horizon estimation for quantized discrete time systems. IEEE Trans Automat Contr 2021; **66**: 4199–205.

[24] Zhu M and Martínez S. On the performance analysis of resilient networked control systems under replay attacks. IEEE Trans Automat Contr 2014; **59**: 804–8.

[25] Farha F, Ning H and Yang S et al. Timestamp scheme to mitigate replay attacks in secure ZigBee networks. IEEE Trans Mob Comput 2022; **21**: 342–51.

[26] Xu Y, Yang L and Wang Z et al. State estimation for networked systems with Markov driven transmission and buffer constraint. IEEE Trans Syst Man Cybern Syst 2021; **51**: 7727–34.

[27] Zhang H, Cheng P and Shi L et al. Optimal dos attack scheduling in wireless networked control system. IEEE Trans Control Syst Technol 2016; **24**: 843–52.

[28] Mo Y and Sinopoli B. Secure control against replay attacks. In: 2009 47th Annual Allerton Conference on Communication, Control, and Computing, Allerton, 2009, 911–8.

[29] Dan Y, Tyz A and Ge G. Stochastic coding detection scheme in cyber-physical systems against replay attack. Inform Sci 2019; **481**: 432–44.

[30] Ferrari RMG and Teixeira AMH. Detection and isolation of replay attacks through sensor watermarking. In: IFAC-PapersOnLine, 6–8 July 2016, Boston, MA, USA, **Vol. 50**, 2017, 7363–68.

[31] Chen Y, Kar S and Moura JMF. Cyber-physical attacks with control objectives. IEEE Trans Automat Contr 2018; **63**: 1418–25.

[32] Wu G and Jian S. Optimal data integrity attack on actuators in cyber-physical systems. In: Proceedings of the 2016 American Control Conference, 9–14 July 2017, Toulouse, 2016.

[33] Liang L, Xing H and Lei D et al. Exploring adversarial attack in spiking neural networks with spike-compatible gradient. In: IEEE Transactions on Neural Networks and Learning Systems, 2021, in press. https://doi.org/10.1109/TNNLS.2021.3106961.

[34] Başar T and Olsder GJ. Dynamic Noncooperative Game Theory. Philadelphia: SIAM, 1998.

[35] Başar T and Bernhard P. H-Infinity Optimal Control and Related Minimax Design Problems: A Dynamic Game Approach. Berlin: Springer Science & Business Media, 2008.

[36] Dorf RC and Bishop RH. Modern Control Systems, twelfth edition. Upper Saddle River, NJ: Pearson Prentice Hall, 2015.

Sheng Gao received his B.Sc. degree in automation from Donghua University, Shanghai, China in 2019. He is currently working toward the Ph.D. degree in control science and engineering at Tongji University, Shanghai, China. His current research interests include optimal control, cyber-physical systems, robot, and cyber security.

Hao Zhang received her B.Sc. degree in automatic control from Wuhan University of Technology, Wuhan, China, in 2001 and received her Ph.D. degree in control theory and control engineering from Huazhong University of Science and Technology Wuhan, China, in 2007. Currently, she is a professor with the School of Electronic and Information Engineering, Tongji University, Shanghai, China. Her research interests include network-based control systems, multi-agent systems, and autonomous systems.

Zhuping Wang received her B.Eng. and M.Eng. degrees from the Department of Automatic Control in 1994 and 1997, respectively, both from Northwestern Polytechnic University, China, and her Ph.D. degree from National University of Singapore in 2003. Currently, she is a professor at the College of Electronics and Information Engineering, Tongji University, Shanghai, China. Her research interests include intelligent control of robotic systems, self-driving vehicles, and nonholonomic control systems.

Chao Huang received his B.Sc., M.Sc., and Ph.D. degrees from Zhejiang University, in 2010, 2012, and 2015, respectively, all in Electrical Engineering. In 2016, he was a post-doctoral research fellow at the School of Engineering, the Australian National University. From 2017 to 2019, he was with the School of Automation, Hangzhou Dianzi University, as a lecturer. He is now with the School of Electronics and Information Engineering, Tongji University, where he is currently an assistant professor. His research interests include system identification, nonlinear and adaptive control, and multi-agent systems.