2025 IEEE/SICE International Symposium on System Integration (SII)
January 21-24, 2025, Munich, Germany

Detection and Cancellation of Multiplicative FDI Attack on Bilateral Encrypted Control System in Variable Periodic Motion

Katsumasa Kosha[1,†], Tetsuro Miyazaki[1,†], Kaoru Teranishi[2,3], Kiminao Kogiso[4], and Kenji Kawashima[1]

Abstract— **Teleoperation of remote assist robots has recently advanced owing to the development of communication technology. However, anonymous malicious attacks may intercept or falsify the network control system. Therefore, it is necessary to improve the security against cyber-attacks. As a countermeasure, an encrypted control method has been applied to prevent intercepting and detect the falsification of control parameters, as well as control signals by performing control operations with encrypted signals and parameters. Furthermore, we have proposed the algorithm to detect and restore the attack exploiting a vulnerability of encryption, which falsifies the plaintext by multiplying a constant factor. However, the algorithm is only effective for periodic motions with a fixed operating frequency and amplitude. If the frequency or amplitude of the motion is smaller than those of the base motion, the algorithm cannot detect the attack. To solve the problem, we propose an improved algorithm to detect and restore the attack in periodic motion with variable operating frequency and amplitude. In the proposed method, the operating frequency and amplitude are obtained through the position frequency analysis. They contribute to update the base energy, which is the average energy of corresponding periodic motion. We verified the proposed method for the bilateral control system using ElGamal encryption and experimentally confirmed its effectiveness against the FDI attack in various periodic motion.**

I. INTRODUCTION

Recently, research on remote robot control has increased owing to the development in communication technology. Bilateral control is a method that enables teleoperation [1], [2], [3], and it involves an operator-controlled device known as the leader device and a remotely located device known as the follower device. When both the leader and follower devices are coupled by sending reference values, control that follows each other's position and force is achieved. This facilitates remote control while receiving external force feedback; thus it it critical in tasks requiring precise force perception, such as surgical assistance.

In such remote control systems, it is critical to establish security against cyber-attacks [4], [5], [6], [7]. Missing a malicious attack on the control system can result in serious consequences. A prevalent form of attack on control systems is the False Data Injection (FDI), which involves falsifying signals and control commands over the network; thus, enabling unauthorized manipulation or destruction of the control target.

As an effective countermeasure against cyber-attacks on control systems, encrypted control has been proposed in [8], [9], and it involves encrypting control parameters and signals. In encrypted control, homomorphic encryption [10] is used to compute the controller's output from the encrypted control parameters and encrypted controller's inputs, thereby hiding the parameters and signals of the control system. Moreover, encrypted control is sensitive to data falsification. Owing to encryption properties, decrypting falsified ciphertext generates significant white noise in the decrypted controller's output [11], which can facilitate the detection of several FDI attacks.

However, there is the malleability of encryption schemes used in encrypted control [12], [13]. For example, in ElGamal encryption [14], malleability allows the plaintext to be manipulated by multiplying the second component of the ciphertext by a constant. There have been several studies on detecting attacks on encrypted control [15], [16], [17], [18]. The authors proposed a detection method using an energy index to detect the FDI attack exploiting the malleability, and verified experimentally the effectiveness. Nevertheless, these studies only focus on detection, and restoring the attacks is outside the scope. In [19], an algorithm was proposed to detect and cancel the impact of the FDI attack exploiting one of the vulnerabilities of the encryption. The algorithm monitors the energy increase caused by the attack and estimates the attack parameters by signal processing that exploits the encryption property. However, the algorithm only assumes that the input motion is periodic with a fixed frequency and amplitude, so it is not valid with different frequencies or amplitudes. In particular, when the operating frequency or amplitude is small, the algorithm cannot catch up the increase of the energy due to the attack, making it impossible to detect the attack.

This study aims to improve the attack detection and restoration algorithm to be valid in periodic motion with variable frequencies and amplitudes. This study considers the updating of the base energies, M_l and M_f, which are used in calculation of the monitor index, γ_l and γ_f. The updates uses a polynomial approximation of the base energy by the operating frequency and amplitude online. This update mechanism is the novelty of this study, which is the extension

*This work was supported in part by KAKENHI under Grant JP22H01509 and JP23K22779.

[1]Department of Information Physics and Computing, The University of Tokyo, 7-3-1 Hongo, Bunkyo-ku, Tokyo 113-8656, Japan katsumac50@g.ecc.u-tokyo.ac.jp, Tetsuro_Miyazaki@ipc.i.u-tokyo.ac.jp, Kenji_Kawashima@ipc.i.u-tokyo.ac.jp

[2]Oden Institute for Computational Engineering and Sciences, The University of Texas at Austin, Austin, Texas, USA teranishi@utexas.edu

[3]Japan Society for the Promotion of Science, Chiyoda, Tokyo, Japan

[4]Department of Mechanical and Intelligent Systems Engineering, The University of Electro-Communications, 1-5-1 Chofugaoka, Chofu-shi, Tokyo 182-8585, Japan kogiso@uec.ac.jp

†Equal contribution

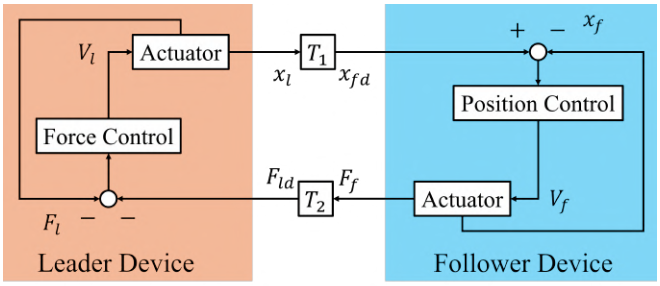


Fig. 1: Block diagram of the entire control system. The leader device sends the position signal to the follower device, and the follower device sends the force signal to the leader device.

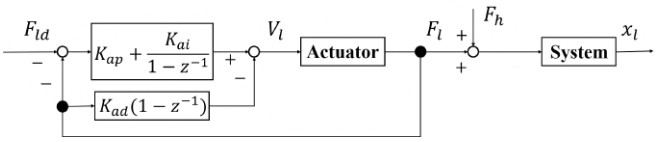


Fig. 2: Block diagram of the leader device. Calculate the control voltage from the reference signal of the cylinder force.

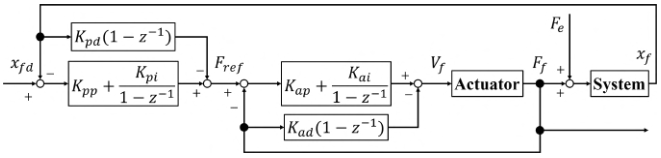


Fig. 3: Block diagram of the follower device. Calculate the control voltage from the reference signal of the cylinder position.

of [19]. The frequency and amplitude are obtained realtime through the position frequency analysis. The effectiveness of the proposed attack detection and restoration method in periodic motion with variable frequencies and amplitudes are validated experimentally.

This paper is organized as follows. Section II introduces the concept of encrypted control to describe the attack model for the bilateral encrypted control system. Section III proposes the modification of the base energy using the position frequency analysis. Section IV demonstrates the effectiveness of the proposed method though experiments under several cases. Finally, Section V concludes this paper.

Notations: $\mathbb{Z}$ denotes the set of integers, and $\mathbb{Z}_{\geq i}$ denotes the set of integers greater than or equal to $i \in \mathbb{Z}$. The variables in this study include discrete time variables, which are shown with the step $k \in \mathbb{Z}_{\geq 0}$. $(\cdot)^{l\times n}$ indicates a matrix with l rows and n columns. $\dot{(\cdot)}$ indicates the differential value of variable $(\cdot)$.

II. PROBLEM SETUP

A. FORCE-FEEDBACK BILATERAL CONTROL

This section describes the bilateral control system used in this study. Fig. 1 shows the block diagram of the entire control system based on [19]. The leader device sends its position, x_l to the follower device, and the follower device sends its force, F_f to the leader device. The control requirements are considered as follows: $x_l = x_f, \quad F_l = -F_f$, where x_f is the follower position and F_l is the leader force.

There exists a time delay in the communication between each device [20]. As shown in Fig. 1, if the reference force of the leader is F_{ld}, the reference position of the follower is x_{fd}, and the time delay steps T_1, T_2 between the leader and follower, then the following relationship holds:$x_{fd}(k) = x_l(k-T_1), \quad F_{ld}(k) = F_f(k-T_2)$.

The control block diagrams of the leader and follower devices included in Fig. 1 are shown in Figs. 2 and 3, respectively. The leader device performs the force control, which calculates the control voltage, V_l from F_{ld}, and V_l is input to the actuator. In Fig. 2, K_{ap}, K_{ai}, and K_{ad} are the force proportional gain, force integral gain, and force differential gain, respectively. z is z-transformation operator.

In this study, the leader's motion is a periodic motion with frequency f and amplitude A, which is moved by the human hand. F_h indicates the force on the actuator by the operator. The position, x_l, is sent to the follower device.

The follower device performs the cascade control, that is, the position control, including the force control inside. The controller calculates the control voltage, V_f from x_{fd}, and V_f is input to the actuator. As shown in Fig. 3, K_{pp}, K_{pi}, and K_{pd} are the position proportional gain, position integral gain, and position differential gain, respectively. F_e indicates the external force on the follower device by contact with such an obstacle. The force, F_f, is sent to the leader device.

B. ENCRYPTED CONTROL

In this study, we implemented encryption in a bilateral control system based on [19]. As encryption scheme, the encrypted control used Elgamal encryption [14]. ElGamal encryption is multiplicative homomorphic encryption that conceals the control parameters and signals. ElGamal encryption scheme, which is denoted as $\mathscr{E}^{\times}$, consists of Gen: $p \mapsto (\mathrm{pk}, \mathrm{sk}) = ((\mathbb{G}, q, g, h), s)$, Enc:$(\mathrm{pk}, m) \mapsto c = (c_1, c_2) = (g^r \bmod p, mh^r \bmod p)$, and Dec:$(\mathrm{sk}, c) \mapsto m' = c_1^{-s} c_2 \bmod p$, where $p = 2q+1$ is a safe prime. g is a generator of a cyclic group $\mathbb{G} = \{g^i \bmod p | i \in \mathbb{Z}_q\}$ such that $g^q \bmod p = 1$: s is a random number in $\mathbb{Z}_q$ generated once by the keygen: r is a random number $\mathbb{Z}_q$ in generated for every encryption instance. : and $h = g^s \bmod p$, where $\mathbb{Z}_q = \{0, 1, 2, \cdots, q-1\}$. The plaintext and ciphertext spaces, $\mathscr{M}$ and $\mathscr{C}$, are expressed by $\mathscr{M} = \mathbb{G}$ and $\mathscr{C} = \mathbb{G}^2$, respectively. ElGamal encryption has multiplicative homomorphism as follows:

$$\begin{aligned} &\mathrm{Dec}(\mathrm{sk}, \mathrm{Enc}(\mathrm{pk}, m) * \mathrm{Enc}(\mathrm{pk}, m') \bmod p) \\ &\qquad = mm' \bmod p, \end{aligned} \tag{1}$$

where $\forall m, m' \in \mathscr{M}$, and $*$ represents the Hadamard product. This property allows the preservation of multiplication over encrypted data.

The overview of the encrypted control system is shown in Fig. 4. Enc and Dec^+ denote encryption and decryption,

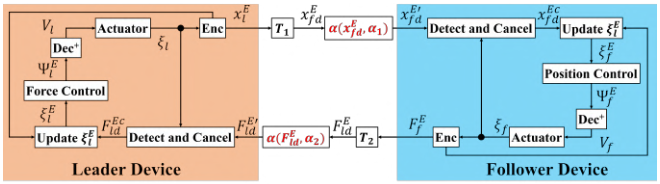


Fig. 4: Block diagram of encrypted bilateral control system. The superscript E indicates that the variable is encrypted. V_l and V_f are calculated on ciphertext space $\mathscr{C}$.

respectively. The superscript E indicates that the variable is encrypted. In the leader device, the state vector, ξ_l is encrypted to $\xi_l^E = \mathrm{Enc}(\mathrm{pk}, \xi_l)$, and updated with F_{ld}^E, which is conducted in Update ξ_l^E block in Fig. 4. Ψ_l^E is calculated with ξ_l^E, which is used to calculate the control voltage, V_l. This is the same on the follower side.

The implementation of the encrypted control allows us to hide the reference value on the communication channel, control the voltage of each device, and calculate the contents of the reference value. The computational domain in plaintext is only the control voltage input to the device and drive. In encrypted control, the control law is expressed as follows: $\boldsymbol{\psi} = f(\boldsymbol{\Phi}, \boldsymbol{\xi}) = \boldsymbol{\Phi}\boldsymbol{\xi}$, where $\boldsymbol{\Phi} = [\boldsymbol{\Phi}_1 \ \boldsymbol{\Phi}_2 \ \cdots \ \boldsymbol{\Phi}_n] \in \mathbb{R}^{l \times n}$ is the coefficient matrix that arranges the parameters of the controller, and $\boldsymbol{\xi} = [\xi_1 \ \xi_2 \ \cdots \ \xi_n]^\top \in \mathbb{R}^n$ is the state vector that lays out the control signal. The control computation can be divided into multiplication and addition, such as $f = f^+ \circ f^\times$, where $f^\times$ and f^+ are denoted as follows: $f^\times(\boldsymbol{\Phi}, \boldsymbol{\xi}) = [\boldsymbol{\Phi}_1\xi_1 \boldsymbol{\Phi}_2\xi_2 \ \cdots \ \boldsymbol{\Phi}_n\xi_n] = \boldsymbol{\Psi}, f^+(\boldsymbol{\Psi}) = \sum_{k=1}^n \boldsymbol{\Psi}_k = \psi$. The ciphertext corresponding to ψ_{ij} can be calculated directly as $\mathrm{Enc}(\mathrm{pk}, \Phi_{ij})\mathrm{Enc}(\mathrm{pk}, \xi_j) \bmod p$ owing to multiplicative homomorphism (1). However, ψ cannot be calculated as a ciphertext owing to addition. Therefore, ψ is obtained after decrypting each component of $\mathrm{Enc}(\mathrm{pk}, \boldsymbol{\Psi})$ and adding them together. Defining $\mathrm{Dec}^+ = f^+ \circ \mathrm{Dec}$, it holds that $\psi = \mathrm{Dec}^+(\mathrm{sk}, \mathrm{Enc}(\mathrm{pk}, \boldsymbol{\Psi}))$. To conduct the encrypted control, $\boldsymbol{\Phi}$ and ξ, which are real numbers, must be conversed to the components of $\mathscr{M}$. This study employs the mapping used in [15]. Based on the above discussion, we implemented the encrypted control in bilateral control [19].

C. ATTACK MODEL

This study considered the FDI attack under the assumption that the attackers know that the ElGamal encryption scheme is used for the encrypted control system and can access the network of the bilateral control system unauthorized. The attack exploits malleability in the ElGamal encryption, and an attack function $a : \mathscr{C} \times \mathbb{Z}_{\geq 2} \to \mathscr{C}$ is introduced as follows,

$$a(c(k), \alpha) = (c_1, \alpha c_2 \bmod p), \quad \forall k \geq K, \tag{2}$$

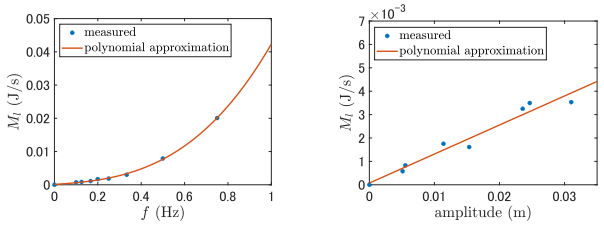
where $\alpha \in \mathbb{Z}_{\geq 2}$ and $K \in \mathbb{Z}_{\geq 0}$ are an attack parameter and a step when the attack starts, respectively. The multiplication of c_2 by α results in manipulating a corresponding plaintext m, i.e., $\mathrm{Dec}(a(c, \alpha)) = \alpha m$.

The bilateral control system involving the FDI attacks in (2) is shown in Fig. 4. The blocks, $a(x_{fd}^E, \alpha_1)$ and $a(F_{ld}^E, \alpha_2)$,

Algorithm 1 Detect and Cancel Algorithm

Require: $c(k) \in \{F_{ld}^{E'}(k), x_{fd}^{E'}(k)\}$,
$\sigma(k) \in \{0,1,2,3\}$, $\hat{\alpha}(k)$, $\bar{\gamma}$, $k \in \mathbb{Z}_{\geq 0}$
$\mathscr{H} = \{\mathscr{H}_l, \mathscr{H}_f\}$,
$\mathscr{H}_l = \{\dot{x}_l(0), \cdots, \dot{x}_l(k), F_l(0), \cdots, F_l(k)\}$,
$\mathscr{H}_f = \{\dot{x}_f(0), \cdots, \dot{x}_f(k), F_f(0), \cdots, F_f(k)\}$
Ensure: $c_c(k)$, $\sigma(k+1)$, $\hat{\alpha}(k+1)$, $\bar{\gamma}$

```
if k mod Ival == 0 then
    X(f) = FT(x(k − T_F + 1) − x_0, ··· , x(k) − x_0)
    amp(f) = |X(f)|
    A = max(amp(f))
    f = argmax(amp(f))
    r_A = g_amp(A)/M_0
    r_f = g_freq(f)/M_0
    M = r_A r_f M_0
end if
γ(k) ← RMS(k)/M
if σ(k) == 0 then
    CheckGamma(c(k), γ(k))
else if σ(k) == 1 then
    EstimateAttackParam(c(k), γ̄)
else if σ(k) == 2 then
    CancelAttack(c(k), γ(k), α̂(k))
else if σ(k) == 3 then
    ModifyAttackParam(c(k), α̂(k), γ̄)
end if
```



(a) Base energy M_l at each operating frequency and polynomial curve (3rd order)

(b) Base energy M_l at each operating amplitude and polynomial curve (1st order)

Fig. 5: Change in base energy M_l.

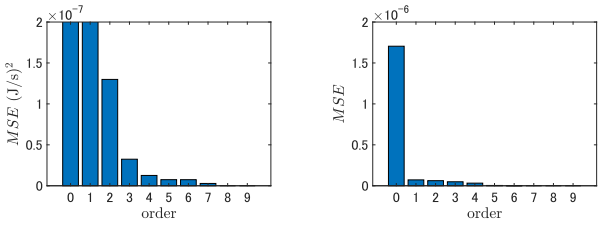
are the functions that falsify the references in ciphertext. The attacks correspond to the manipulation of the original plaintexts as follows,

$$\mathrm{Dec}(x_{fd}^{E'}(k)) = \alpha_1 x_{fd}(k), \ \mathrm{Dec}(F_{ld}^{E'}(k)) = \alpha_2 F_{ld}(k), \tag{3}$$

where $x_{fd}^{E'}$ and $F_{ld}^{E'}$ are the falsified references ciphertext, and $\alpha_i \in \mathbb{Z}_{\geq 2}$, $\forall i \in \mathscr{I} := \{1,2\}$ are the attack parameters. This causes the impairing of tracking performance without the operator noticing.

III. PROPOSED METHOD

This section proposes the algorithm of updating the base energy using position frequency analysis to improve the attack detection and restoration, compared with [19]. The proposed algorithm is shown in **Algorithm 1**. In the previous study, they utilized the base energy, M_0 in the periodic



(a) MSE at each orders between measured base energy and the estimated vale by the approximation in frequency

(b) MSE at each orders between measured base energy and the estimated vale by the approximation in amplitude

Fig. 6: MSE between measured base energy and the estimated value by the approximation at each order.

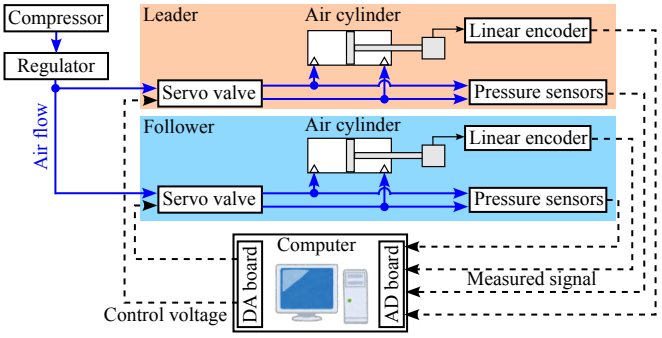


Fig. 7: Pneumatic circuit and control systems of the experimental setup.

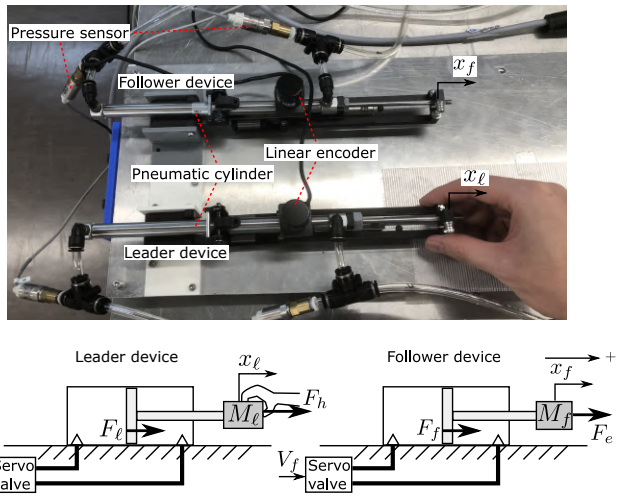


Fig. 8: Overview and schematic diagrams of the leader and follower devices consisting of masses and pneumatic cylinders.

motion with the base frequency f_0 and base amplitude A_0. The base energy is the average energy of corresponding periodic motion. In this study, the algorithm updates the base energy, M_0 using f and A obtained through position frequency analysis in lines 1 to 10. As shown in line 1, the update is conducted every $Ival$ step. In line 2, the algorithm converts the time series data of the position, $[x(k-T_F+1)-x_0,\cdots,x(k)-x_0]$ to the frequency domain, $X(f)$ by the Fourier Transform(FT). x_0 is the mean of $[x(k-T_F+1),\cdots,x(k)]$. In line 3, the amplitude spectrum, $|X(f)|$ is calculated, assigned to $amp(f)$. In lines 4 and 5, it obtains the operating frequency, f, and the operating amplitude, A from $amp(f)$. A is assigned the maximum value of $amp(f)$, and f is assigned the corresponding frequency. In line 6 to 8, M is updated using polynomial approximation, as follows: the approximation by operating frequency, $g_{freq}(f)$, and one by operating amplitude, $g_{amp}(A)$. Using these approximate curves, this algorithm calculates the ratio of the base energy, M_0 calculated offline. $r_A = g_{amp}(A)/M_0$ is the ratio of M_0 due to the change in A, and $r_f = g_{freq}(f)/M_0$ is that due to the change in f. In line 8, it updates the base energy to $r_A r_f M_0$. For ease of calculation, this study treats the impact of f on M and that of A separately. However, their effects on M are not strictly independent since the base energy M is calculated using the velocity and force, and the f and A determine the velocity. We will treat this issue in our future work. In line 10, calculates γ using the updated M.

Fig. 5 shows the relationship between the base energy of the leader, M_l and f and A. The blue dots indicate the measured values, and the orange curve is the polynomial approximation. Fig. 6 shows the results of MSE between each base energy and the estimated value by the approximation when learning at each order. As the order increases, MSE decreases, and the smallest orders where the decrease is less than 10 % of the MSE of the last order are the third order in frequency and the first order in amplitude. The order should be as small as possible because the computational load are small, and a higher order can cause overfitting. Therefore, the order of $g_{freq}(f)$ is three, $g_{freq}(f) = c_{f0} + c_{f1} f + c_{f2} f^2 + c_{f3} f^3$, and the order of $g_{amp}(A)$ is one, $g_{amp}(A) = c_{A0} + c_{A1} A$. Each coefficient was determined by the least squares method using the measured values and the polynomials, $g_{freq}(f)$ and $g_{amp}(A)$.

IV. EXPERIMENT

A. EXPERIMENTAL SETUP

The pneumatic circuit and control systems in our experiments are shown in Fig. 7, where blue lines indicate airflow and black dotted lines represent electrical signals. The leader and follower devices of the constructed bilateral control system were one-degree-of-freedom, single-rod pneumatic cylinders of identical structure, as shown in Fig. 8.

Linear encoders and pressure sensors measure the position and pressure of the leader and follower devices. The control voltages, V_l and V_f, are calculated using the sensor values, and then input to the servo valves. The leader device was set up for force control, while the follower device managed position control, which incorporated aspects of force control. The servo valves adjusted the pneumatic cylinder pressures based on the control voltages. An operator periodically maneuvered the leader device with frequency f and amplitude A, while pneumatic pressure actuates the follower device.

Parameter values used in the experiments are listed in TABLE I. The parameters were decided experimentally by trial and error.

TABLE I: Experimental parameters.

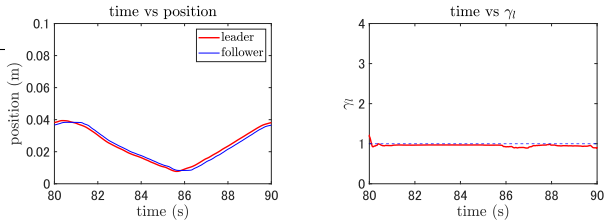
Sampling frequency [Hz]	1000
Supplied Pressure [kPa]	250
Communication delay step (Leader to Follower) T_1	25 (0.025 s)
Communication delay step (Follower to Leader) T_2	25 (0.025 s)
Length of key [bit]	64
Force proportional gain (Leader) K_{ap} [V/N]	1.0
Force integral gain (Leader) K_{ai} [V/(N·s)]	0.2
Force differential gain (Leader) K_{ad} [V·s/N]	0.0
Force proportional gain (Follower) K_{ap} [V/N]	1.0
Force integral gain (Follower) K_{ai} [V/(N·s)]	0.2
Force differential gain (Follower) K_{ad} [V·s/N]	0.0
Position proportional gain (Follower) K_{pp} [N/m]	900.0
Position integral gain (Follower) K_{pi} [N/(m·s)]	20.0
Position differential gain (Follower) K_{pd} [N·s/m]	0.0
Motion base frequency f_0 [Hz]	0.25
Motion base amplitude A_0 [m]	0.025
Interval step of update M	5000 (5.000 s)
Polynomial coefficient ($g_{freq}(f)$, 0th order) c_{f0} [J/(s)]	1.088×10^{-4}
Polynomial coefficient ($g_{freq}(f)$, 1st order) c_{f1} [J/(s·Hz)]	4.253×10^{-3}
Polynomial coefficient ($g_{freq}(f)$, 2nd order) c_{f2} [J/(s·Hz^2)]	5.661×10^{-3}
Polynomial coefficient ($g_{freq}(f)$, 3rd order) c_{f3} [J/(s·Hz^3)]	3.232×10^{-2}
Polynomial coefficient ($g_{amp}(A)$, 0th order) c_{A0} [J/(s)]	3.030×10^{-4}
Polynomial coefficient ($g_{amp}(A)$, 1st order) c_{A1} [J/(s·m)]	0.1277

TABLE II: Type and nature of attacks conducted in the experiment.

Attack scenario	Contents
(i) $\alpha_1 = 1, \alpha_2 = 1$	Confirm the behavior of γ_l at lower frequency from f_0.
(ii) $\alpha_1 = 1, \alpha_2 = 1$	Confirm the behavior of γ_l at smaller amplitude from A_0.
(iii) $\alpha_1 = 1, \alpha_2 = 2$	Doubling the encrypted reference F_{ld} at lower frequency, in which the detection method is the conventional.
(iv) $\alpha_1 = 1, \alpha_2 = 2$	Doubling the encrypted reference F_{ld} at lower frequency , in which the detection method is the proposed.
(v) $\alpha_1 = 1, \alpha_2 = 2$	Doubling the encrypted reference F_{ld} at smaller amplitude , in which the detection method is the proposed.

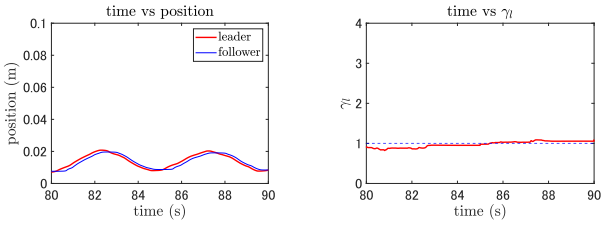
B. VERIFICATION CASE

The detailed verification cases are outlined in TABLE II. Our experiments considered the attacks on the encrypted reference of the leader, $F_{ld}^{E'}$. The experiments explored the following cases: (i) $\alpha_1 = 1$, $\alpha_2 = 1$: No attack is simulated to verify the behavior of γ_l on periodic motion with a lower frequency, f = 0.1 than f_0; (ii) $\alpha_1 = 1$, $\alpha_2 = 1$: No attack is simulated to verify the behavior of γ_l on periodic motion with a smaller amplitude, A = 0.005 than A_0; (iii) $\alpha_1 = 1$, $\alpha_2 = 2$: The attacker falsifies the leader's reference force, F_{ld} to twice its intended value on periodic motion with $f = 0.1 \leq f_0$ and $A = A_0$. In this case, the attack detection was attempted using the conventional method [19]; (iv) $\alpha_1 = 1$, $\alpha_2 = 2$: The attacker falsifies the leader's reference force, F_{ld} to twice its intended value on periodic motion with $f = 0.1 \leq f_0$ and $A = A_0$ with the proposed method.; (v) $\alpha_1 = 1$, $\alpha_2 = 2$: The attacker falsifies the leader's reference force, F_{ld} to twice its intended value on periodic motion with $f = f_0$ and $A = 0.005 \leq A_0$. In (iv) and (v), the attack detection was attempted using the proposed method. The FDI attacks were executed every step according to (3) and commenced at 90 s after the operation begins.



(a) cylinder positions x_l and x_f (b) index γ_l

Fig. 9: Results of the attack scenario (i): There is no attack.



(a) cylinder positions x_l and x_f (b) index γ_l

Fig. 10: Results of the attack scenario (ii): There is no attack.

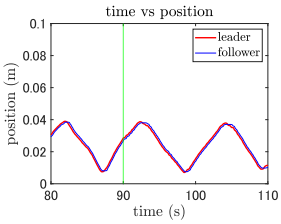
C. RESULT

The experimental results of the verification cases (i)-(v) are shown in Figs. 9-13, respectively. In Figs. 9 and 10, subfigures (a) and (b) display time resposes of position and index γ_l, respectively. In Figs. 11, 12, and 13, subfigures (a)-(f) display time responses of position, velocity, and force of the cylinder, index, status, and estimation of attack parameters, respectively. In these figures, the red and blue lines represent the leader and follower, respectively. The green lines in Figs. 11, 12, and 13 marks the start of the attack at 90 s. The magenta broken line indicates the threshold of γ_l for detection.

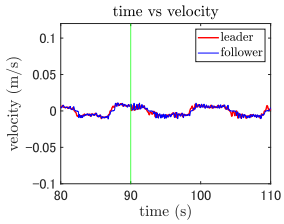
According to Fig. 9, the leader device moved periodically with $f = 0.1 \leq f_0$ and $A = A_0$. The follower device was controlled to track the leader's position. Fig. 9b displays that γ_l hovered around one, although the operating frequency was different from the base frequency.

According to Fig. 10, the leader device moved periodically with $f = f_0$ and $A = 0.005 \leq A_0$. The follower device was controlled to track the leader's position. Fig. 10b displays that γ_l hovered around one, although the operating amplitude was different from the base amplitude. Consequently, this result shows that the impact of changes in operating frequency and amplitude can be corrected by modifying M_l using polynomial approximation.

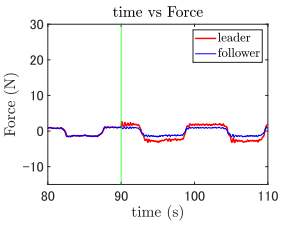
Fig. 11 shows the results of the attack detection in lower frequency motion without the proposed method. Fig. 11c depicts that the force of the leader was manipulated to be twice the value of the force of the follower owing to the attack (3). According to Fig. 11d, γ_l hovered lower than one due to the input motion with the lower frequency than the base motion. It resulted in failing the detection of the attack although γ_l increased owing to the FDI attack, shown



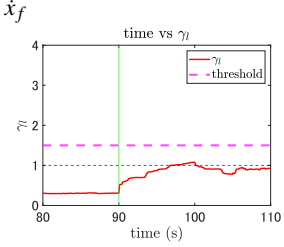
(a) cylinder positions x_l and x_f



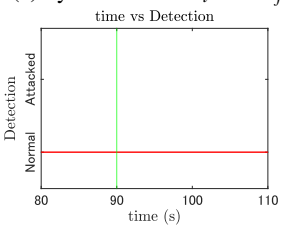
(b) cylinder velocities $\dot{x}_l$ and $\dot{x}_f$



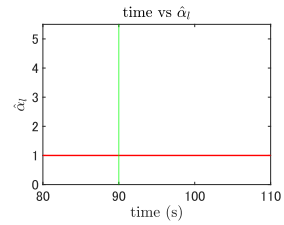
(c) cylinder force F_l and F_f



(d) index γ_l

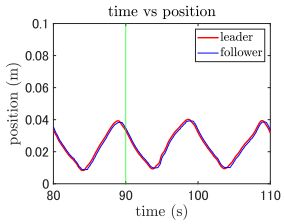


(e) status *st*

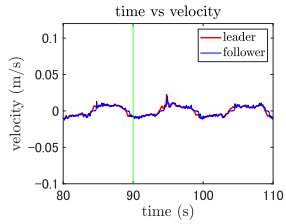


(f) $\hat{\alpha}_2$

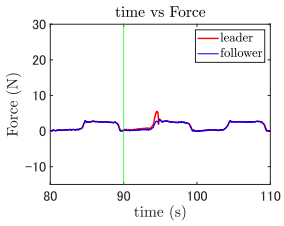
Fig. 11: Results of attack scenario (iii).



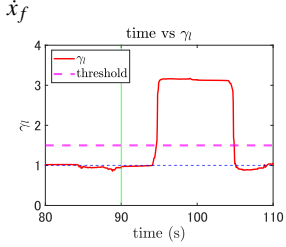
(a) cylinder positions x_l and x_f



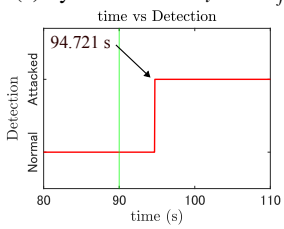
(b) cylinder velocities $\dot{x}_l$ and $\dot{x}_f$



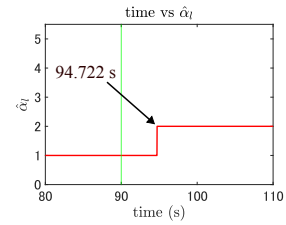
(c) cylinder force F_l and F_f



(d) index γ_l



(e) status *st*



(f) $\hat{\alpha}_2$

Fig. 12: Results of attack scenario (iv).

in Fig. 11e. This case confirmed that the previous method cannot detect the FDI attacks in the input motion with lower frequency than the base motion, which is the same for the amplitude.

Fig. 12 illustrates that the follower device was controlled to track the position of the leader, while the leader force was manipulated to be twice the value of the force of the follower owing to the attack (3). Fig. 12d indicates that before the attack began, γ_l hovered around one regardless of the periodic motion with lower frequency. It was due to the modification of M_l described in (i). After the attack began, γ_l approached 3.0 and returned to approximately one in 10 s (the window width). Fig. 12e shows that after the attack initiation, 4.721 s, the algorithm detected it as the status changed to *Attacked*, and the falsified reference was subsequently modified as demonstrated in Fig. 12f. Consequently, confirming that the algorithm could detect and cancel the impact of the attack on periodic motion with different frequency from the base frequency.

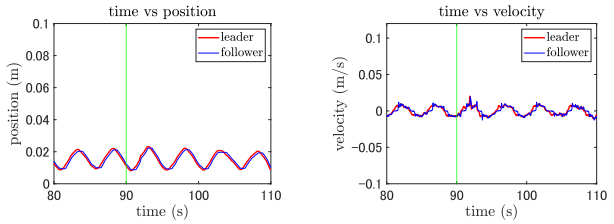
Fig. 13 also illustrates that the follower device was controlled to track the position of the leader, while the leader force was manipulated to be twice the value of the force of the follower owing to the attack (3). Fig. 13d indicates that before the attack began, γ_l hovered around one regardless of the periodic motion with smaller amplitude. It was due to the modification of M_l described in (ii). After the attack began, γ_l approached 3.0 and returned to approximately one in 10 s. Fig. 13e shows that after the attack initiation, 1.805 s, the algorithm detected it as the status changed to *Attacked*, and the falsified reference was subsequently modified as demonstrated in Fig. 13f. Consequently, confirming that the algorithm could detect and cancel the impact of the attack on periodic motion with different amplitude from the base amplitude.

Finally, a discussion on computation costs. The mean of computation times for the update process shown in lines 1-9 of **Algorithm. 1** were as follows: 10.22 ms in case (iv) and 10.05 ms in case (v). In this study, while the sampling time was 1 ms, the update process was performed once per 5000 ms, which is sufficiently longer than the update process. As shown in the experimental results, it was confirmed that the computational cost does not significantly affect the control performance.

The experimental results validated that the proposed algorithm can modify M_l due to the changes of the operating frequency and amplitude, leading to detecting and canceling the impact of the attack on periodic motion with various frequency and amplitude.

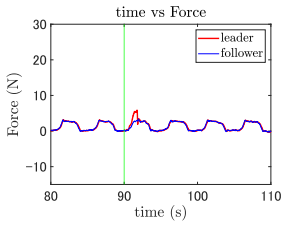
V. CONCLUSION

This study proposed the improved algorithm to detect and restore FDI attacks on periodic motion with various frequency and amplitude. In the previous study [19], the algorithm only assumes that the input motion is periodic with a fixed frequency and amplitude, so it is not valid with different requencies or amplitudes. The proposed algorithm

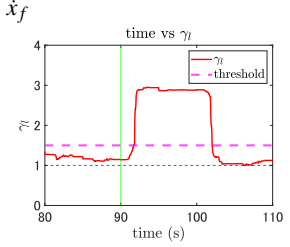


(a) cylinder positions x_l and x_f

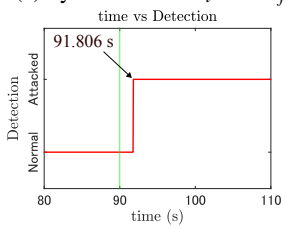
(b) cylinder velocities $\dot{x}_l$ and $\dot{x}_f$



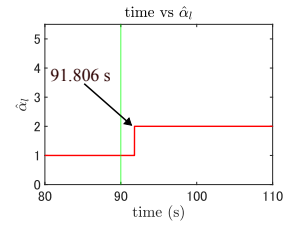
(c) cylinder force F_l and F_f



(d) index γ_l



(e) status *st*



(f) $\hat{\alpha}_2$

Fig. 13: Results of attack scenario (v).

modifies the base energy, M_l and M_f, using polynomial approximation of the energy by operation frequency and amplitude, obtained through position frequency analysis. The authors confirmed that the algorithm could modify the base energy correctly and detect and cancel the impact of the attack on periodic motion with various frequency and amplitude; thus leading to expanding applicability of the detection algorithm.

In future work, the authors will refine the proposed algorithm to further enhance system security and usability. This will include more accurate correction by polynomial approximation and reducing implementation effort. It is expected that resolving these issues will lead to the realization of more secure and user-friendly cyber-physical systems.

References

[1] T. B. Sheridan, "Telerobotics," *Automatica*, vol. 25, no. 4, pp. 487-507, 1989, DOI: 10.1016/0005-1098(89)90093-9.

[2] T. B. Sheridan, "Space teleoperation through time delay: Review and prognosis," *IEEE Transactions on Robotics and Automation*, vol. 9, no. 5, pp. 592-606, 1993, DOI: 10.1109/70.258052.

[3] P. F. Hokayem and M. W. Spong, "Bilateral teleoperation: An historical survey," *Automatica*, vol. 42, no. 12, pp. 2035-2057, 2006, DOI: 10.1016/j.automatica.2006.06.027.

[4] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *in Proc. 2008 28th International Conference on Distributed Computing Systems Workshops*, pp. 495-500, Jun. 2008, DOI: 10.1109/ICDCS.Workshops.2008.40.

[5] M. S. Chong, H. Sandberg, and A. M. H. Teixeira, "A tutorial introduction to security and privacy for cyber-physical systems," *in Proc. 2019 18th European Control Conference (ECC)*, pp. 968-978, Jun. 2019, DOI: 10.23919/ECC.2019.8795652.

[6] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 9, pp. 52-80, 2015, DOI: 10.1016/j.ijcip.2015.02.002.

[7] J. Ueda and J. Blevins, "Affine transformation-based perfectly undetectable false data injection attacks on remote manipulator kinematic control with attack detector", *IEEE Robotics and Automation Letters*, vol. 9, no. 10, pp. 8690-8697, Oct. 2024, DOI: 10.1109/LRA.2024.3451397.

[8] K. Kogiso and T. Fujita, "Cyber-security enhancement of networked control systems using homomorphic encryption," *in Proc. 2015 54th IEEE Conference on Decision and Control (CDC)*, pp. 6836-6843, Dec. 2015, DOI: 10.1109/CDC.2015.7403296.

[9] M. S. Darup, A. B. Alexandru, D. E. Quevedo, and G. J. Pappas, "Encrypted control for networked systems: An illustrative introduction and current challenges," *IEEE Control Systems Magazine*, vol. 41, no. 3, pp. 58-78, 2021, DOI: 10.1109/MCS.2021.3062956.

[10] J. H. Cheon, A. Kim, M. Kim, Y. Song, "Homomorphic encryption for arithmetic of approximate numbers," *in Proc. Advances in Cryptology — ASIACRYPT 2017*, pp. 409-437, Dec. 2017, DOI: 978-3-319-70694-8_15.

[11] K. Kogiso, "Attack detection and prevention for encrypted control systems by application of switching-key management," *in Proc. 2018 IEEE Conference on Decision and Control (CDC)*, pp. 5032-5037, Dec. 2018, DOI: 10.1109/CDC.2018.8619221.

[12] J. Katz and Y. Lindell, *Introduction to Modern Cryptography, Third Edition*, UK: Chapman and Hall/CRC, 2020.

[13] K. Teranishi and K. Kogiso, "Control-theoretic approach to malleability cancellation by attacked signal normalization," *IFAC-PapersOnLine*, vol. 52, no. 20, pp. 297-302, 2019, DOI: 10.1016/j.ifacol.2019.12.171.

[14] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, July 1985, DOI: 10.1109/TIT.1985.1057074.

[15] N. Shono, T. Miyazaki, K. Teranishi, T. Kanno, T. Kawase, K. Kogiso, and K. Kawashima, "Implementation of encrypted control of pneumatic bilateral control system using wave variables," *in Proc. 27th International Symposium on Artificial Life and Robotics*, AROB OS13-1, Jan. 2022.

[16] N. Shono, T. Miyazaki, K. Teranishi, K. Kogiso, and K. Kawashima, "A false data injection attack model targeting passivity of encrypted wave variable based bilateral control system," *in Proc. 2023 IEEE/SICE International Symposium on System Integration (SII)*, pp. 1-6, Jan. 2023, DOI: 10.1109/SII55687.2023.10039338.

[17] T. Miyazaki, N. Shono, K. Teranishi, T. Kanno, T. Kawase, K. Kogiso, and K. Kawashima, "Attack detection method for encrypted wave-variable-based bilateral control systems," *IET Control Theory & Applications*, vol. 18, pp. 1461-1474, 2024, DOI: 10.1049/cth2.12697.

[18] M. Miyamoto, K. Teranishi, K. Emura, and K. Kogiso, "Cybersecurity-Enhanced Encrypted Control System Using Keyed-Homomorphic Public Key Encryption," *IEEE Access*, vol. 11, pp. 45749-45760, 2023, DOI: 10.1109/ACCESS.2023.3274691.

[19] K. Kosha, T. Miyazaki, K. Teranishi, K. Kogiso, and K. Kawashima, "Detection and cancellation of multiplicative FDI attack on bilateral encrypted control system," *IEEE Access*, vol. 12, pp. 120979-120993, 2024, DOI: 10.1109/ACCESS.2024.3438287

[20] W. R. Ferrell, "Delayed force feedback," *Human Factors*, vol. 8, no. 5, pp. 449-455, 1966, DOI: 10.1177/001872086600800509.