IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 5 August 2022, accepted 13 September 2022, date of publication 21 September 2022, date of current version 29 September 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3208232

RESEARCH ARTICLE

Real-Time Controller Reconfiguration for Delay-Resilient Cyber-Physical Systems

SANGJUN KIM[1], SANGHOON LEE[2], AND KYUNG-JOON PARK[2], (Senior Member, IEEE)
[1]Korea Research Institute for Defense Technology Planning and Advancement (KRIT), Jinju-si 52851, Republic of Korea
[2]Department of Electrical Engineering and Computer Science, DGIST, Daegu 42988, Republic of Korea

Corresponding author: Kyung-Joon Park (kjp@dgist.ac.kr)

This work was supported by the Future Combat System Network Technology Research Center Program of Defense Acquisition Program Administration and Agency for Defense Development under Grant UD190033ED.

ABSTRACT Networks on the cyber-physical systems (CPSs) configure feedback control loops between physical systems in the real world and control software in the cyber world. Malicious behaviors on the networks can increase network delays by exhausting limited network resources and security vulnerabilities to destabilize CPSs, which are entitled the network delay attack. In this paper, we focus on the problem of how to guarantee the stability of CPS under the network delay attack. We propose a real-time controller reconfiguration to ensure the resiliency of the physical systems against the network delay attack. Our controller reconfiguration consists of two algorithms: controller gain tuning and access point (AP) handover, which give a delay tolerance and an attack avoidance, respectively. Depending on the network delays, the computing system adopts one of these two algorithms and mitigates the physical impacts of the network delay attack. We validate that the proposed controller reconfiguration can ensure the resiliency of CPS against the network delay attack by implementing a testbed with wireless networks.

INDEX TERMS Attack-resilient CPS, controller reconfiguration, cyber-physical systems, flooding attack.

I. INTRODUCTION

Networks on the cyber-physical systems (CPSs) connect the real and cyber world, where the physical systems in the real world and computing systems in the cyber world interact by exchanging packets [1], [2]. With the advancement in communication technologies, sensors, and actuators on the physical systems support real-time wireless communications, which configure remote connections to the computing systems. Introducing the wireless networks in the CPS has more advantages for maintenance cost reduction, energy-saving, and mobility than conventional wired control systems [3]. Therefore, wireless networks are the key component in industrial CPSs, such as industrial control systems, intelligent transport systems, and various societal infrastructure (e.g., water distribution systems).

Feedback control over wireless networks is a time-critical CPS application, where the control input signals and sensor measurements are periodically transmitted through the networks in a certain packet format [4]. Over the wireless networks, CPSs conduct feedback control, which exchanges sensor measurement for physical system monitoring in the computing systems and control input signals for actuating the physical systems as a user intention [5]. In the viewpoint of the control theory, sensing and actuating delays affect control performance of the physical systems, where the network delays for exchanging sensor measurements and control input signals are dominant [6], [7].

However, wireless networks have limited network resources and inherent security vulnerabilities [8], [9]. The malicious attacker can easily access the wireless networks from the security vulnerabilities and can inject various network attacks to disturb interactions between physical and computing systems. For instance, network delay attacks, implemented by exhausting limited network resources, remotely impede the transmissions of sensor measurements and control input signals. Resulting of network delay attacks, attack-induced network delays disrupt the physical systems

The associate editor coordinating the review of this manuscript and approving it for publication was Gyorgy Eigner.

without physical damage. Therefore, a resilient CPS design strategy is essential to ensure the stability of the physical systems under network delay attacks [10].

In this paper, we first analyze the impact of network delay attacks that violate the stability conditions of the physical systems. Then, we derive the maximum allowable delay bound of the feedback control system. We propose a resilient controller reconfiguration based on the physical impact analysis with the delay bound to handle network delay attacks in wireless networks. The proposed controller reconfiguration consists of two attack handling algorithms: *controller gain tuning* and *access point (AP) handover*. If the attack-induced network delay remains in the feasible stability region, the controller gain tuning algorithm provides delay tolerance to the physical systems. Otherwise, the AP handover algorithm neutralizes network delay attacks by reconstructing a new control loop with another computing system. The main contributions of the paper are summarized as follows:

- We analyze the stability condition of CPS with time-varying network delays. Then, we derive the maximum allowable delay bound for the stability region.
- We propose a *real-time* resilient controller reconfiguration against the network delay attack. The proposed approach provides a delay-aware controller reconfiguration to ensure the stability of CPS.
- We conduct an empirical study to validate the performance of the proposed controller reconfiguration by implementing a testbed with wireless networks. The experimental results show that the proposed controller reconfiguration ensures the stability of the physical system against network delay attacks.

The remainder of the paper is organized as follows: In Section II, we discuss related work on wireless networked control systems (NCSs) and the effects of network delay attacks on CPSs. Section III provides the mathematical models of CPSs and an analysis of the maximum allowable delay bound of the feedback control systems. In Section IV, we propose a controller reconfiguration for delay-resiliency of CPSs. We empirically evaluate the network delay attack mitigation performance of the proposed controller reconfiguration in Section V. Finally, Section VI presents the conclusion.

II. RELATED WORK

A. PHYSICAL IMPACTS OF NETWORK DELAYS IN CPS

Network delays on CPSs degrade the control performance and affect the stability of physical systems. In control theory, CPSs are modeled as NCSs consisting of physical systems, feedback controllers, and networks, where the feedback control is conducted through the networks [9].

The impact of network delays on CPSs is traditionally analyzed in control-theoretic approaches using a mathematical NCS model. A physical impact of constant delays is analyzed in [11] and provides the stability region of an NCS model. The authors in [12] presented a physical impact of the time-varying network delays of NCSs to reflect the realistic network on NCSs, where a sequence of delays in the stability region can destabilize NCSs. Furthermore, the stability analysis of [12] shows that the stability condition depends on the controller design in computing systems and the sampling period of the physical systems. An empirical study in [13] showed the impact of network delay attacks over a wireless network for a realistic drone control system. The study [13] considered the network delay attack as consumption of limited network resources, which is implemented as the Internet control message protocol (ICMP) flooding attack that transmits large ICMP packets within a short time interval. The experimental results in [13] showed that network delays by the ICMP flooding attack incur time-outs of sensor measurement deliveries, resulting in the activation of fail-safe mode on the drone system.

B. CONTROLLER RECONFIGURATION AGAINST CYBER ATTACKS

Controller reconfiguration techniques make control systems robust against cyber attacks and system faults. However, most of studies mainly focus on the sensor and actuator faults, or simple communication failure. In [14], a fault-tolerant control mechanism for power systems is proposed against sensor measurement failure. The proposed control mechanism augments legitimate sensor measurements to provide state estimation when the observability of control systems is lost by sensor faults or communication errors. Authors in [15] propose a virtual actuator method with a reconfiguration block in the feedback control loop, which does not require modification of the original controller. In [15], the power system has redundant actuators, and the VA method redirects control signals to the redundant actuators when actuation faults are detected. Furthermore, the study in [16] extends the VA methods in [15] into multi-input multi-output (MIMO) control systems. When a certain actuator suffers from failure, the VA method in [16] redistributes control input signals to other available actuators, which is independent to the actuator redundancy [15]. Both VA methods in [15] and [16] mitigate physical effects on the actuator fault, and show a better settling time than the case without the VA.

For network delay attacks, most conventional studies consider network delays as constant. A fuzzy control method is proposed in [17], which simultaneously considers physical states and communication delays to ensure the stability of the control systems. The proposed method divides communication latency into three sections, and provide proper control input signals to mitigate the delay effect in physical systems. The study [18] proposed a piece-wise constant control technique for recovering control performance against various cyber-physical attacks, including a constant network delay attack. The proposed control technique estimates the effect of cyber-physical attacks and generates control input signals to stabilize the physical systems under the attacks by solving a linear programming problem. In [19], a machine learning (ML)-based safety guaranteeing strategy was proposed for power grid systems under a constant delay attack.

The proposed strategy consists of an ML-based safety checking algorithm and two attack mitigation methods; proportional-integral-derivative (PID) controller gain adjustment and load shedding. If the PID gain adjustment is impossible to stabilize the power grid systems, the proposed strategy sheds the load of the systems.

A robust controller design mechanism is proposed in [20] against network delays and model uncertainty for power systems. The authors in [20] show that the proposed controller stabilizes the power system under bounded time-varying delays. The study [21] proposed a sampling rate optimization to mitigate the delay effect of an NCS with massive physical systems. Furthermore, study [21] formulated a physical instability by network delays as a network saturation problem and proposes a convex optimization problem considering control performance and network energies.

Conventional controller reconfiguration methods mainly consider a control theoretical perspective. However, both control theory and networks should be considered at the same time against network delay attacks. To mitigate the physical impact of network delay attacks, in this paper, our controller reconfiguration provides a controller gain tuning algorithm and AP handover in the viewpoints of control theory and network knowledge, respectively. Furthermore, most of studies considers network delays as a constant value, which is not practical in realistic CPSs with wired/wireless networks. We evaluate our controller reconfiguration in the testbed with realistic wireless networks, which shows attack mitigation performance under time-varying delays.

III. PHYSICAL IMPACT OF NETWORK DELAY ATTACKS

In this section, we analyze the impact of network delay attacks on the physical system from the stability viewpoint. We employ the NCS model proposed in [12] under time-varying network delays and derive the maximum allowable delay bound. The maximum allowable delay bound provides a stability region of the physical system by changing feedback controller gains. The stability region in our proposed controller reconfiguration is a criterion to select between controller gain tuning and AP handover after network delay attack detection.

A. NETWORKED CONTROL SYSTEM MODEL

We simplify the CPS as an NCS consisting of a physical system, network, and computing system, as shown in Fig. 1. As a physical system, we consider a linear time-invariant (LTI) system in the continuous time domain given by

$$\dot{x}(t) = Ax(t) + Bu(t), \tag{1}$$

where $x(k) \in \mathbb{R}^n$ is the state of the physical system with n dimension; $A \in \mathbb{R}^{n\times n}$ is the system matrix; $B \in \mathbb{R}^n$ is the input matrix; $u(t) \in \mathbb{R}$ is the control input signal. For the LTI system (1), we assume that a matrix pair (A, B) is controllable.

The feedback control in CPS is conducted by exchanging the physical state $x(t)$ and the control input signal $u(t)$ in a certain packet format. Therefore, the physical system (1) should

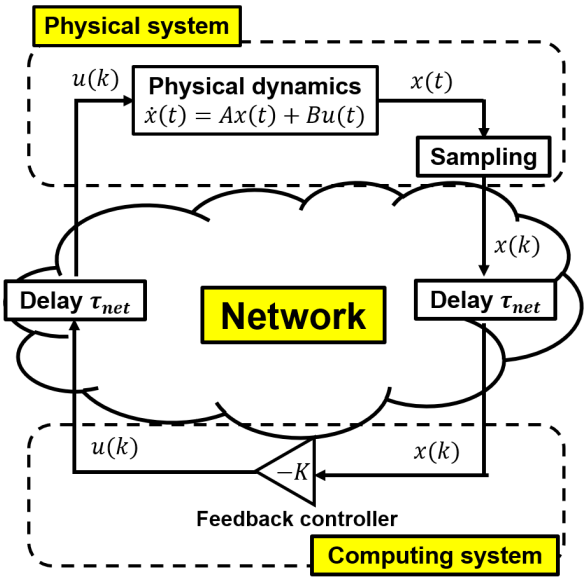

FIGURE 1. Structure of a networked control system.

be controlled in the discrete-time domain. We consider a full-state feedback control system with a single control input signal $u(t)$ in discrete-time domain with sampling period t_s. The sensors on the physical system periodically collect and transmit the physical state $x(k)$ in every time step k. Then, the computing system calculates and returns the control input signal $u(k)$. The discrete-time model of the feedback control system with zero-order hold is given as follows:

$$\begin{aligned} x(k+1) &= A_d x(k) + B_d u(k), \\ u(k) &= -Kx(k), \end{aligned} \tag{2}$$

where A_d is the system matrix in the discrete-time domain; B_d is the input matrix in the discrete-time domain; $K \in \mathbb{R}^{1\times n}$ is the controller gain in the computing system. We assume that the controller gain K is appropriately selected to place the poles of the closed-loop control system model (2), i.e., poles of the matrix $A_d - B_d K$ lie in a unit circle [22].

To utilize the NCS model under time-varying network delay proposed in [12], we consider the bound in the network delays τ_{net} between minimum delay bound τ_{min} and maximum delay bound τ_{max}. We denote the time instant t_j^k as follows:

$$\begin{aligned} t_j^k = min\{\, & max\left\{0, \tau_{k+j-\bar{d}} + (j-\bar{d})t_s\right\}, \\ & max\left\{0, \tau_{k+j-\bar{d}+1} + (j-\bar{d}+1)t_s\right\}, \cdots, \\ & max\left\{0, \tau_{k-\bar{d}} - \underline{d}t_s\right\}, t_s\,\}, \end{aligned}$$

where $0 = t_0^k < \cdots < t_j^k < t_{j+1}^k < \cdots < t_{\bar{d}-\underline{d}+1}^k = t_s$. From the time instant t_j^k, we rewrite the discrete-time NCS model (2) as follows:

$$x(k+1) = A_d x(k) + \sum_{j=0}^{\bar{d}-\underline{d}} \int_{t_s - t_{j+1}^k}^{t_s - t_j^k} e^{As} ds B u(k+j-\bar{d}), \tag{3}$$

where $\underline{d} \triangleq \lfloor \tau_{min}/t_s \rfloor$ and $\bar{d} \triangleq \lceil \tau_{max}/t_s \rceil$. The revised NCS model (3) shows that the current physical state $x(k)$ depends on the current control input signal $u(k)$ and the previous control input signals due to the network delay τ_{net}.

To describe the behavior of the state $x(k)$ under delayed control input signals, we introduce ξ dynamics in the state space form as follows:

$$\xi(k+1) = \tilde{A}(\boldsymbol{t}^k)\xi(k) + \tilde{B}(\boldsymbol{t}^k)u(k), \tag{4}$$

where $\xi(k) \triangleq \left[x(k)^T u(k)^T u(k-1)^T \cdots x(k-\bar{d})^T\right]^T$ is the augmented state vector with physical state $x(k)$ and delayed control inputs. For more details for matrices $\tilde{A}(\boldsymbol{t}^k)$ and $\tilde{B}(\boldsymbol{t}^k)$ in the state space of ξ dynamics (4), see [12].

B. MAXIMUM ALLOWABLE DELAY BOUND OF NCS

The matrices $\tilde{A}(\boldsymbol{t}^k)$ and $\tilde{B}(\boldsymbol{t}^k)$ in the ξ dynamics (4) have an infinite number of conditions because of time instant set $\boldsymbol{t}^k$, making it hard to analyze precise state $x(t)$ under the network delay. The number of conditions for the matrices $\tilde{A}(\boldsymbol{t}^k)$ and $\tilde{B}(\boldsymbol{t}^k)$ should be limited to analyze the stability bound of the NCS model (3) in finite time.

By over-approximation of the matrices $\tilde{A}(\boldsymbol{t}^k)$ and $\tilde{B}(\boldsymbol{t}^k)$ in [12], we present a set of these matrices as linear combinations as follows:

$$\mathcal{H}_{FG} = \left\{ \left(F_0 + \sum_{i=1}^{v}\sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j}F_{i,j},\ G_0 + \sum_{i=1}^{v}\sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j}G_{i,j} \right) : \alpha_{i,j} \in \left\{\underline{\alpha}_{i,j}, \bar{\alpha}_{i,j}\right\}, i=1,\cdots,v, j=1,\cdots,\bar{d}-\underline{d} \right\}, \tag{5}$$

where $F_0, G_0, F_{i,j}$, and $G_{i,j}$ are constant matrices decomposed by the Jordan form; $\alpha_i(t_j^k)$ is a time-varying function for continuous time instant t_j^k. Details for v and $\alpha_i(t_j^k)$ in (5) are described in [23]. Additionally, the upper and lower bounds of the time-varying function $\alpha_i(t_j^k)$ are defined as $\bar{\alpha}_{i,j} \triangleq max_{t_j^k \in [t_{min}^k, t_{max}^k]}\alpha_i(t_j^k)$ and $\underline{\alpha}_{i,j} \triangleq min_{t_j^k \in [t_{min}^k, t_{max}^k]}\alpha_i(t_j^k)$ with time instants

$$t_{j,min} = \begin{cases} \tau_{min} - \underline{d}t_s & \text{if } j = \bar{d}-\underline{d} \\ 0, & \text{if } 1 \le j < \bar{d}-\underline{d}, \end{cases}$$

$$t_{j,max} = \begin{cases} t_s, & \text{if } 1 < j \le \bar{d}-\underline{d} \\ \tau_{max} - \underline{d}t_s & \text{if } j = 1. \end{cases}$$

The sets $H_F \triangleq \left\{F_0 + \sum_{i=1}^{v}\sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j}F_{i,j}\right\}$ and $H_G \triangleq \left\{G_0 + \sum_{i=1}^{v}\sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j}G_{i,j}\right\}$ correspond to time-varying matrices $\tilde{A}(\boldsymbol{t}^k)$ and $\tilde{B}(\boldsymbol{t}^k)$ in ξ dynamics (4), respectively.

For all matrix pairs $\mathcal{H}_{FG}$ under bounded network delays $\tau_{net} \in [\tau_{min}, \tau_{max}]$, we can verify the destabilization of the physical system by solving linear matrix inequalities (LMIs) as follows:

$$\begin{pmatrix} P & \left(H_F - H_G\bar{K}\right)^T P \\ P\left(H_F - H_G\bar{K}\right) & P \end{pmatrix} > 0, \tag{6}$$

where $\bar{K} \triangleq \left[K\ 0_{1,\bar{d}}\right]$. If a positive definite matrix P exists in LMIs (6) for a given controller gain K, the NCS in (3) ensures the stability under the attack-induced delays $\tau'_{net} < \tau_{max}$ [12].

IV. DELAY-AWARE CONTROLLER RECONFIGURATION

In this section, we propose a delay-aware controller reconfiguration under network delay attacks. We consider a DC motor position control system as an example of a physical system. Based on the analysis of the physical system for network delays, we describe details of the controller reconfiguration with two algorithms: *controller gain tuning* and *AP handover*.

The controller gain tuning algorithm makes physical systems delay-tolerant by enlarging the maximum allowable delay bound τ_{max} exceeding the attack-induced delay τ'_{net}, providing seamless control to the feedback control system. The AP handover algorithm replaces the controller with a new one by re-establishing the control loop of the physical system; thereby, neutralizing the attack. Furthermore, we assume that the CPS has multiple wireless networks and computing systems to apply the AP handover in the proposed controller reconfiguration.

A. DC MOTOR CONTROL UNDER NETWORK DELAYS

We consider the well-known DC motor position control system as a physical system [24]. The control object is to regulate the angle of the DC motor to zero by adjusting the input voltage. We adopt the second-order LTI model of the DC motor position control system as follows:

$$\begin{aligned} \dot{\mathbf{x}}(t) &= \begin{bmatrix} 0 & 1 \\ 0 & \frac{-k_m^2 k_g^2}{R_m(J_m k_g^2 + J_l)} \end{bmatrix} \mathbf{x}(t) \\ &\quad + \begin{bmatrix} 0 \\ \frac{k_m k_g}{R_m(J_m k_g^2 + J_l)} \end{bmatrix} u(t), \\ u(t) &= -K\mathbf{x}(t), \end{aligned} \tag{7}$$

where $\mathbf{x}(t) = \left[\theta(t)\ \dot{\theta}(t)\right]^T$ is the state vector of the DC motor system; $\theta(t)$ is the motor angle; k_m is the back-electromotive force constant; k_g is the gear ratio; J_m is the motor inertia; J_l is the load inertia; R_m is the motor armature resistance. In the motor system in (7), our main focus is on the stability of the physical system. In addition, we do not consider the limitation of control input signals and state variables in order to show the state divergence of the physical system due to network delay attacks. For networks, we assume that all state variables on the physical system (7) are aggregated in a packet, and are transmitted at once. Therefore, simultaneously sampled state variables at a certain time have the same network delay τ_{net}.

We analyze the maximum allowable delay bound of the DC motor position control system model (7) using LMIs (6). Fig. 2 shows the stability region of the DC motor position control system analyzed using LMIs (6). Here, we numerically evaluate the delay bound τ_{max} by changing controller gain $K = [k_1\ k_2]$.

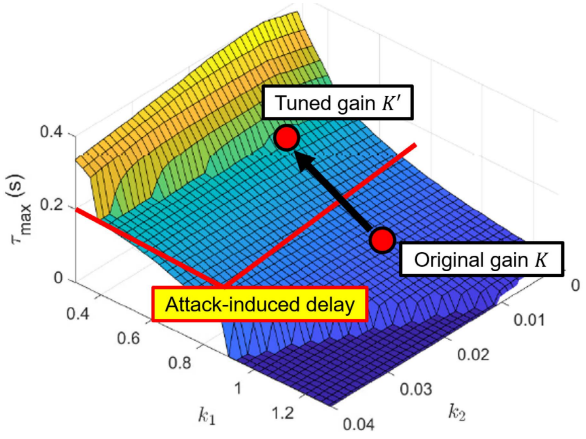

FIGURE 2. Controller gain tuning mechanism with respect to maximum allowable delay bound of DC motor control system.

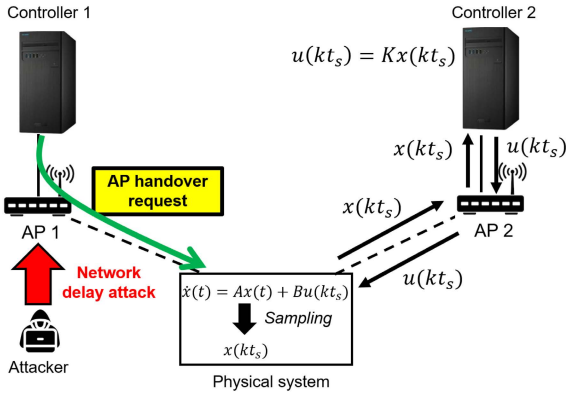

FIGURE 3. Access point handover algorithm.

The delay bound analysis illustrated in Fig. 2 shows that there is a trade-off between control performance and delay tolerance. Generally, a high-gain controller provides faster state tracking speed than a low-gain controller. However, the high-gain controller provides a lower maximum allowable delay bound τ_{max} than a low-gain controller, as shown in Fig 2.

B. CONTROLLER GAIN TUNING

The network delay attacks impede transmissions of sensor measurements and control input signals. The physical systems are destabilized when attack-induced delays exceed the maximum allowable delay bound derived from (6). The trade-off between control performance and delay tolerance illustrated in Fig. 2 shows that the delay bound of the physical system can be enhanced by tuning the controller gain K.

Here, we assume that the computing systems measure the network delays using a suitable method. As shown in Fig. 2, the computing system cannot guarantee the stability of the physical system when the attack-induced delay τ'_{net} exceeds the delay bound of controller gain K. Meanwhile, when the network delay attacks are detected, the computing systems guarantee the stability of the physical system by replacing the controller gain K into the new controller gain K' that has a larger delay bound than the attack-induced delay τ'_{net}. The controller gain tuning algorithm selects the gain K' by solving the following optimization problem:

$$\begin{aligned} &Find \quad K', \\ &s.t. \ \left|\lambda\left(A_d - B_d K'\right)\right| < 1, \\ &\quad \tau'_{max} > \tau'_{net}, \\ &\quad \begin{pmatrix} P & \left(H_F - H_G\bar{K}'\right)^T \\ P\left(H_F - H_G\bar{K}'\right) & P \end{pmatrix} > 0. \end{aligned} \tag{8}$$

Here, $\lambda(\cdot)$ is the eigenvalue of the matrix; τ'_{net} is the attack-induced network delay; τ'_{max} is the updated maximum allowable delay bound with the new controller gain K'. The physical impact of the attack-induced delays τ'_{net} can be mitigated by enhanced maximum allowable delay bound τ'_{max} from the updated controller gain K'.

The controller gain tuning algorithm has no network overheads from a change of the sampling period t_s or temporal network disconnection for a network policy update. Therefore, the controller gain tuning algorithm can provide seamless network delay attack mitigation with a fixed sampling period t_s. It is worth noting that the controller gain tuning algorithm reduces the control performance of the physical systems because of the trade-off between control performance and delay tolerance, as shown in Fig 2.

C. ACCESS POINT (AP) HANDOVER

When attack-induced delay τ'_{net} is beyond the stability region, the controller gain tuning algorithm cannot ensure the stability of the physical systems. In this case, the controller gain selection problem (8) has no solution. Then, we execute the AP handover algorithm to replace the computing system with a new one to maintain the stability of the physical system.

We assume that there are two computing systems and two APs, as shown in Fig 3, where the physical system is connected to controller 1 through AP 1. When the attack-induced delay τ'_{net} is beyond the stability region, the computing system 1 tries to solve the problem (8). However, no controller gain can stabilize the physical system under the attack-induced delay τ'_{net}. Then, the controller 1 requests an AP handover to the physical system. The physical system disconnects the original link with AP 1 and tries to access AP 2. Finally, the physical system configures a new feedback control loop to the computing system 2. The network handover eliminates the attack-induced delay τ'_{net} to neutralize the physical impact of attack-induced delay τ'_{net}.

We define a network overhead as the duration from the time the physical emulator receives an AP handover command from computing system 1 to the time it receives the first control input signal from the computing system 2. The AP handover mechanism has some network overheads that degrade the control performance. In the AP handover request procedure, the AP handover request packet suffers

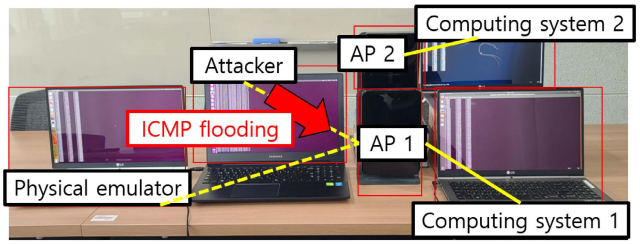

FIGURE 4. Resilient controller reconfiguration testbed.

the attack-induced network delays τ'_{net}, impeding the AP handover execution on the physical system. Furthermore, the wireless link with computing system 1 is removed during the AP handover. Then, the physical system becomes an open-loop control until the new connection is established with the computing system 2. Therefore, the AP handover procedures must be finished before the physical system becomes unstable.

V. PERFORMANCE EVALUATION

In this section, we evaluate the resiliency of the proposed controller reconfiguration under the network delay attack. We implement a wireless NCS testbed, as shown in Fig. 4. Then, we validate the control performance recovery of the physical system for controller gain tuning and AP handover.

A. TESTBED ENVIRONMENT

We implement a wireless NCS testbed. The testbed consists of a physical system emulator [25], two computing systems, two APs, and an attacker, as shown in Fig. 4. The physical system emulator, computing systems, and attacker are implemented in PCs. We embed DC motor position dynamics (7) in the physical emulator to sample and send the physical state $x(kt_s)$ to the computing system in every sampling period t_s. Then, the computing system connected to the physical system emulator calculates and returns the control input signal $u(kt_s)$ to the physical system emulator. We use IEEE 802.11 wireless networks with two APs, where the state $x(kt_s)$ and the control input signal $u(kt_s)$ are delivered by user datagram protocol (UDP) packets. These two APs use physically different wireless channels to avoid the interference of the ICMP flooding.

We consider a realistic network delay attack as the ICMP flooding [13] that exhausts wireless network resources by emitting large-size ICMP packets with high frequency. When the attacker launches ICMP flooding to the AP 1, as shown in Fig. 4, the network delays increase drastically by the wireless network resource consumption for massive ICMP packets.

We measure the network delays τ_{net} using the round trip time (RTT) of UDP packets for every sensing period t_s in the controller. However, the RTT can be temporarily increased under an attack-free environment because of network jitters by inherent a random access property of IEEE 802.11 wireless networks and channel uncertainty. These RTT noises can activate false-positive attack detection in an attack-free environment. To avoid false-positive detection by these RTT noises, we use the moving average (MA) as follows:

$$RTT_{MA}(k) = \frac{\sum_{i=0}^{W-1} RTT(k-i)}{W},$$

where $RTT(k)$ is the network delay in time step k; $RTT_{MA}(k)$ is the MA of the measured delays; W is the MA window size. From the repetitive trials for the RTT measurements in the testbed, we select the window size W as 3 without the false-positive alarms. The proposed controller determines the intensity of the attack-induced delay τ'_{net} by the $RTT_{MA}(k)$ and selects the algorithm.

B. ATTACK SCENARIOS

We consider two types of ICMP flooding attacks to evaluate the recovery performance of controller gain tuning and AP handover.

1) WHEN THE ATTACK-INDUCED DELAY IS IN THE FEASIBLE STABILITY REGION

The solution to the optimization problem (8) exists if the attack-induced delay τ'_{net} remains in the feasible stability region. Therefore, the computing system replaces the feedback controller gain K with tuned gain K' guaranteeing stability against the attack-induced delay τ'_{net}.

2) WHEN THE ATTACK-INDUCED DELAY IS BEYOND THE STABILITY REGION

However, there is no solution to the optimization problem (8) if the attack-induced delay τ'_{net} is beyond the feasible stability region. Therefore, the controller gain tuning algorithm is insufficient to ensure the stability of the physical systems. In this case, the computing system 1 sends an AP handover request packet to the physical system emulator. Then, the physical emulator disconnects to the conventional wireless link through AP 1 and attempts access to AP 2. During the AP handover, the physical emulator holds the last control input signal $u(k)$ until it receives a new control input signal from the computing system 2. After the AP handover, the computing system 2 conducts feedback control to recover the control performance of the physical emulator from the damage by the ICMP flooding attack.

C. EXPERIMENTAL RESULTS

1) WHEN THE ATTACK-INDUCED DELAY IS IN THE FEASIBLE STABILITY REGION

First, we analyze the control performance recovery of CPS using the gain tuning algorithm when the attack-induced delay τ'_{net} remains in the stability region. Fig. 5 shows the performance recovery of the DC motor system. The physical emulator runs for $t_f = 25$ s, and we launch the ICMP flooding attack at $t_a = 5$ s. Then, the computing system 1 detects the network delay τ_{net} at $t = 5.6$ s. After the attack detection, the computing system immediately replaces the controller gain K with K' derived from the optimization problem (8).

As shown in the red graph of Fig. 5, the DC motor angle diverges with oscillation by the attack network delay τ'_{net} that

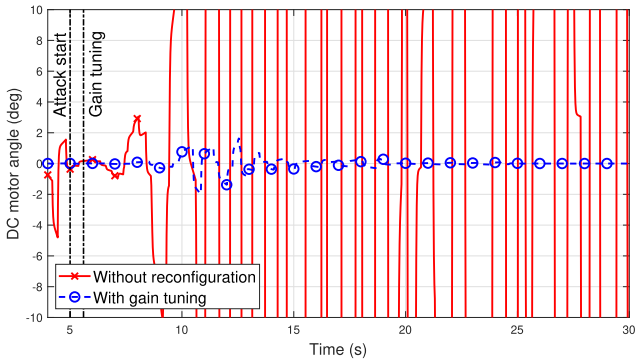

FIGURE 5. Controller gain tuning when the attack-induced delay remains in the feasible stability region.

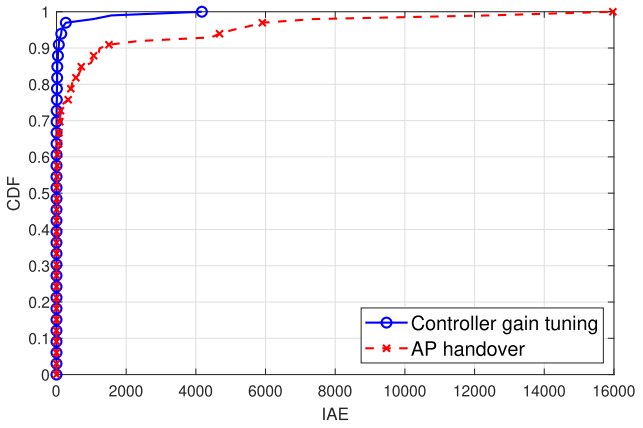

FIGURE 6. Integrated absolute errors of controller gain tuning and AP handover when attack-induced delay remains in the feasible stability region.

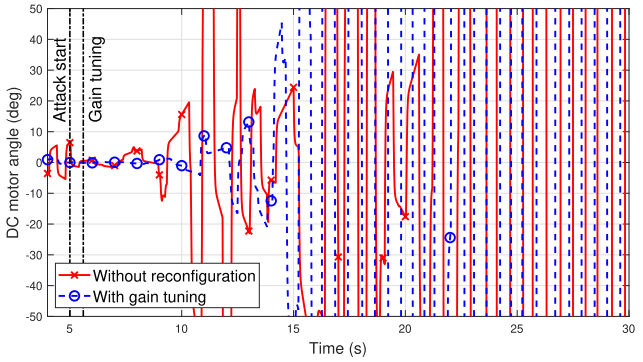

FIGURE 7. Recovery failure when the attack-induced delay is beyond the stability region.

exceeds the delay bound τ_{max}. However, the gain tuning algorithm regulates the DC motor angle to remain around zero, as shown in the blue graph of Fig. 5. The experimental results show that the proposed gain tuning algorithm can ensure the stability of the physical systems when the attack-induced delay τ_{net} is in the feasible stability region.

The AP handover algorithm can also ensure the stability of the DC motor control system. In [26], an AP handover algorithm is activated when a certain attack is detected. However, the DC motor control system temporally becomes an open-loop control state due to the inherent network overhead during AP handover. Therefore, the AP handover algorithm provides poorer recovery performance than the controller gain tuning algorithm. To compare the recovery performance of the proposed controller gain tuning algorithm and the AP handover algorithm in [26], we conduct experiments 100 times for each algorithm.

We use an integrated absolute error (IAE) as a metric to evaluate the recovery performance [25], [27]. IAE is defined as an integral of the absolute value of an error between the DC motor angle $\theta(t)$ and reference angle $\theta_r(t)$. It is calculated as follows:

$$IAE = \int_{t_a}^{t_f} |\theta(t) - \theta_r(t)|\, dt,$$

where t_a is the attack start time; t_f is the experiment time; $\theta_r(t)$ is the reference angle of the DC motor dynamics. Next, we set the reference angle $\theta_r(t) = 0$ based on the control objective mentioned in Section IV. The larger IAE metric indicates poorer recovery performance. We calculate the IAE metric for each experimental result of the controller gain tuning and AP handover algorithms.

Fig. 6 shows the cumulative distribution functions of the IAEs. It shows the recovery performances of the experimental results for the controller gain tuning and AP handover algorithm. The blue graph in Fig. 6 shows that the controller gain tuning algorithm provides better recovery performance than the AP handover algorithm in most cases. The physical system becomes an open-loop state during the network overhead of the AP handover; thereby, degrading the recovery performance. However, the controller gain tuning has no network overhead because the computing system replaces the controller gain. Therefore, the controller gain tuning can provide better recovery performance than the AP handover when the attack-induced delay is in the feasible stability region.

2) WHEN THE ATTACK-INDUCED DELAY IS BEYOND THE STABILITY REGION

If the network delay attack is very intensive, there is no solution to the optimization problem (8). Therefore, the controller gain tuning is insufficient to ensure the stability of the physical system. Fig. 7 shows the recovery failure of the controller gain tuning algorithm when the attack-induced delay is beyond the stability region. The attacker launches the ICMP flooding attack at $t_a = 5$ s, and the controller gain tuning is executed at $t = 5.6$ s. We use the replaced controller gain K' selected in the first scenario.

Fig. 7 shows the divergence of the DC motor angle under intensive network delay attacks in spite of the controller gain tuning. Therefore, the controller gain tuning is limited to control performance recovery. The existence of a solution for the optimization problem (8) determines the execution of the controller gain tuning.

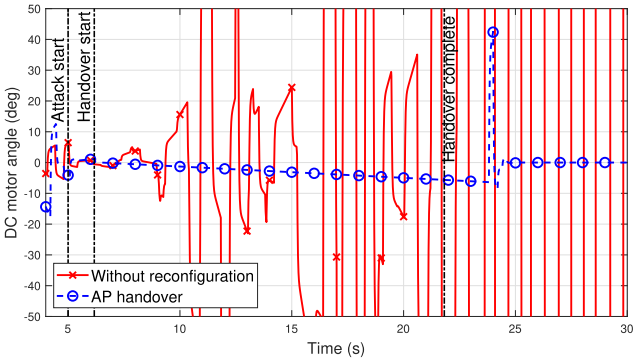

FIGURE 8. AP handover to re-establish the feedback control loop with a new controller.

However, when there is no solution for the optimization problem (8), the computing system 1 sends the AP handover request packet to the physical system. Fig. 8 shows the control performance recovery of the AP handover. The attacker launches the ICMP flooding attack at $t_a = 5$ s, and the physical emulator receives the AP handover request packet from the computing system 1 at $t = 6.17$ s. Then, the physical emulator becomes an open-loop state during the network overhead of 15.65 s and receives a control input signal from the computing system 2 at $t = 21.82$ s. The physical emulator suffers a transient fluctuation immediately after the AP handover because of the impact of the ICMP flooding attack and open-loop state during the network overhead. Then, the DC motor angle is well regulated to zero.

In contrast to the controller gain tuning, the AP handover has a network overhead that degrades the recovery performance. However, the AP handover can neutralize the physical impact of the attack regardless of the level of attack-induced delays.

VI. CONCLUSION

In this paper, we proposed a controller reconfiguration that can ensure the resiliency of CPS against the network delay attack. The proposed controller reconfiguration consists of the controller gain tuning and AP handover algorithm. The selection of these two algorithms is determined by whether the attack-induced delay remains in the stability region or not.

We implemented a testbed and measured the recovery performances by two attack-induced delay scenarios to evaluate the effectiveness of the proposed controller reconfiguration. The experimental results show that the proposed controller reconfiguration can ensure the resiliency of CPS against the intentionally increased network delays. The proposed controller reconfiguration can also enhance the recovery performance more than only AP handover-based attack neutralization when the attack-induced delay is in the feasible stability region.

REFERENCES

[1] K.-J. Park, R. Zheng, and X. Liu, "Cyber-physical systems: Milestones and research challenges," *Comput. Commun.*, vol. 36, no. 1, pp. 1–7, Dec. 2012.

[2] K.-J. Park, J. Kim, H. Lim, and Y. Eun, "Robust path diversity for network quality of service in cyber-physical systems," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2204–2215, Nov. 2014.

[3] H. Song, H. Wen, Q. Yang, J. Tang, Y. Chen, T. Zhang, F. Xie, and S. Chen, "Adaptive secure transmission strategy for industrial wireless edge-enabled CPS," *IEEE Access*, vol. 9, pp. 27287–27297, 2021.

[4] Y. Ma, J. Guo, Y. Wang, A. Chakrabarty, H. Ahn, P. Orlik, and C. Lu, "Optimal dynamic scheduling of wireless networked control systems," in *Proc. 10th ACM/IEEE Int. Conf. Cyber-Phys. Syst.*, Apr. 2019, pp. 77–86.

[5] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[6] W. Zeng and M.-Y. Chow, "A trade-off model for performance and security in secured networked control systems," in *Proc. IEEE Int. Symp. Ind. Electron.*, Jun. 2011, pp. 1997–2002.

[7] M. Zhang, C. Lin, Y. Li, and B. Chen, "Observer design for cyber-physical systems with state delay and sparse sensor attacks," *IEEE Access*, vol. 9, pp. 3261–3268, 2021.

[8] J. Zhu, Y. Zou, and B. Zheng, "Physical-layer security and reliability challenges for industrial wireless sensor networks," *IEEE Access*, vol. 5, pp. 5313–5320, 2017.

[9] D. Kim, Y. Won, Y. Eun, and K.-J. Park, "Resilient architecture for network and control co-design under wireless channel uncertainty in cyber-physical systems," *Trans. Emerg. Telecommun. Technol.*, vol. 30, no. 4, p. e3499, 2019.

[10] S. Kim and K.-J. Park, "A survey on machine-learning based security design for cyber-physical systems," *Appl. Sci.*, vol. 11, no. 12, p. 5458, Jun. 2021.

[11] W. Zhang, M. S. Branicky, and S. M. Phillips, "Stability of networked control systems," *IEEE Control Syst. Mag.*, vol. 21, no. 1, pp. 84–99, Feb. 2001.

[12] M. B. G. Cloosterman, N. V. D. Wouw, W. P. M. H. Heemels, and H. Nijmeijer, "Stability of networked control systems with uncertain time-varying delays," *IEEE Trans. Autom. Control*, vol. 54, no. 7, pp. 1575–1580, Jul. 2009.

[13] Y.-M. Kwon, J. Yu, B.-M. Cho, Y. Eun, and K.-J. Park, "Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles," *IEEE Access*, vol. 6, pp. 43203–43212, 2018.

[14] S. Khosravani, I. N. Moghaddam, A. Afshar, and M. Karrari, "Wide-area measurement-based fault tolerant control of power system during sensor failure," *Electric Power Syst. Res.*, vol. 137, pp. 66–75, Aug. 2016.

[15] M. E. Raoufat, K. Tomsovic, and S. M. Djouadi, "Virtual actuators for wide-area damping control of power systems," *IEEE Trans. Power Syst.*, vol. 31, no. 6, pp. 4703–4711, Nov. 2016.

[16] D. V. Nair and M. S. R. Murty, "Fault tolerant-based virtual actuator design for wide-area damping control in power system," *Electr. Eng.*, vol. 103, no. 1, pp. 463–477, Feb. 2021.

[17] M. Mokhtari, F. Aminifar, D. Nazarpour, and S. Golshannavaz, "Wide-area power oscillation damping with a fuzzy controller compensating the continuous communication delays," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1997–2005, May 2013.

[18] L. Zhang, X. Chen, F. Kong, and A. A. Cardenas, "Real-time attack-recovery for cyber-physical systems using linear approximations," in *Proc. IEEE Real-Time Syst. Symp. (RTSS)*, Dec. 2020, pp. 205–217.

[19] X. Lou, C. Tran, R. Tan, D. K. Y. Yau, Z. T. Kalbarczyk, A. K. Banerjee, and P. Ganesh, "Assessing and mitigating impact of time delay attack: Case studies for power grid controls," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 1, pp. 141–155, Jan. 2020.

[20] M. E. C. Bento, "Fixed low-order wide-area damping controller considering time delays and power system operation uncertainties," *IEEE Trans. Power Syst.*, vol. 35, no. 5, pp. 3918–3926, Sep. 2020.

[21] D. Kim, Y. Won, S. Kim, Y. Eun, K.-J. Park, and K. H. Johansson, "Sampling rate optimization for IEEE 802.11 wireless control systems," in *Proc. 10th ACM/IEEE Int. Conf. Cyber-Phys. Syst.*, Apr. 2019, pp. 87–96.

[22] C.-T. Chen, *Linear System Theory and Design*, 3rd ed. New York, NY, USA: Oxford Univ. Press, 1998.

[23] M. Posthumus-Cloosterman, "Control over communication networks: Modeling, analysis, and synthesis," Ph.D. dissertation, Dept. Mech. Eng., Tech. Univ. Eindhoven, Eindhoven, The Netherlands, 2008.

[24] H. Li, M.-Y. Chow, and Z. Sun, "Optimal stabilizing gain selection for networked control systems with time delays and packet losses," *IEEE Trans. Control Syst. Technol.*, vol. 17, no. 5, pp. 1154–1162, Sep. 2009.
[25] S. Kim, Y. Eun, and K.-J. Park, "Stealthy sensor attack detection and real-time performance recovery for resilient CPS," *IEEE Trans. Ind. Informat.*, vol. 17, no. 11, pp. 7412–7422, Nov. 2021.
[26] B.-M. Cho, S. Kim, K.-D. Kim, and K.-J. Park, "A controller switching mechanism for resilient wireless sensor–actuator networks," *Appl. Sci.*, vol. 12, no. 4, p. 1841, Feb. 2022.
[27] F.-L. Lian, J. Moyne, and D. Tilbury, "Network design consideration for distributed control systems," *IEEE Trans. Control Syst. Technol.*, vol. 10, no. 2, pp. 297–307, Mar. 2002.

SANGJUN KIM received the B.S. degree in electronics engineering from Pukyong National University, Busan, South Korea, in 2017, and the Ph.D. degree in electrical engineering and computer science from the Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, in 2022. He is currently a Researcher with the Korea Research Institute for Defense Technology Planning and Advancement (KRIT), Jinju-si, South Korea. His research interests include security of cyber-physical systems and software defined networking.

SANGHOON LEE received the B.S. degree from the School of Undergraduate Studies, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea, in 2022. He is currently pursing the integrated M.S. and Ph.D. degrees with the Department of Electrical Engineering and Computer Science, DGIST. His research interests include industrial cyber-physical systems and industrial artificial intelligence.

KYUNG-JOON PARK (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering and the Ph.D. degree in electrical engineering and computer science from Seoul National University, Seoul, South Korea, in 1998, 2000, and 2005, respectively. From 2005 to 2006, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2006 to 2010, he was a Postdoctoral Research Associate with the Department of Computer Science, University of Illinois at Urbana–Champaign (UIUC), IL, USA. He is currently a Professor with the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea. His research interests include resilient cyber-physical systems and smart production systems.