IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received October 7, 2021, accepted October 27, 2021, date of publication October 28, 2021, date of current version November 8, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3124024

Dynamic Network Path Provisioning and Selection for the Detection and Mitigation of Data Tampering Attacks in Networked Control Systems

KENTO AIDA, KENTA YAMADA, RYOSUKE HOTCHI, AND RYOGO KUBO, (Member, IEEE)
Department of Electronics and Electrical Engineering, Keio University, Yokohama 223-8522, Japan

Corresponding author: Kento Aida (aida.kento@kbl.elec.keio.ac.jp)

This work was supported in part by JSPS KAKENHI under Grant 18K11275.

ABSTRACT Networked control systems can help build cost-effective and flexible industrial systems. A system that can function while being immune to cyberattacks is necessary. A method called fixed redundant path selection (FRPS) has been proposed to detect and mitigate data tampering attacks in a networked motion control system. This system contains redundant forward network paths from the controller to the motor sides to detect the attacked path by comparing the values that are received through respective paths. Then, a path selector on the motor side chooses a value on the path that is not attacked based on the majority decision. Increasing the number of redundant paths improves the detection performance of simultaneous attacks against multiple paths. However, it also increases the amount of traffic because the same data are transmitted to all of the redundant paths. This study proposes a dynamic redundant path selection (DRPS) method to balance the detection performance and the amount of traffic. The proposed method initially applies three redundant paths and changes the number of redundant paths to five only when the path selector detects a difference among the received values for the three paths. The experiments confirm that the proposed DRPS outperforms the conventional FRPS. The former can detect and mitigate the data tampering attacks while reducing the number of network paths during tampering detection when the system is exposed to simultaneous attacks against up to two of the redundant paths.

INDEX TERMS Cyberattack, cyber-physical system, motion control, networked control system, tampering detection.

I. INTRODUCTION

The Internet of Things (IoT) enables devices to connect to the Internet and communicate with each other. A networked control system (NCS) is an IoT application that can control devices remotely. The NCS consists of a controller, controlled objects, and communication networks. The controller and controlled objects are connected by the communication networks [1]. The NCS has some advantages such as low-cost installation, high-precision control, and high efficiency for large-scale systems [2], [3]. However, the network has communication constraints between the controller and the controlled object. The main constraints include the time delay during the transmission, information loss, and the signal quantization error [4]. In particular, time-delay compensation schemes have been extensively studied [5]–[9]. The detection of system faults in networks, sensors, and actuators can be also considered as possible issues in NCSs [10]–[12]. In addition, the use of public networks increases the chance of cyberattacks against the NCSs [13], [14].

Since most of the current NCSs operate with industry-specific protocols and the operating systems do not connect to external networks, the systems are not exposed to network-related cyberattacks. Recently, NCSs with external connections have been installed and they are exposed to a variety of cyberattacks. This has motivated researchers to address the cybersecurity issues prevalent in NCSs. Paridari *et al.* provided a general framework to analyze the various attack methods in NCSs [15]. Additionally, some researchers have investigated the security frameworks of cyber-physical

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

systems [16]–[19]. The effect of a covert attack, which is one of the critical cyberattacks for NCSs, on cyber-physical systems was discussed in [20] and [21]. Zhou *et al.* [22] proposed an attack detection algorithm for smart grids and indicated the security risks in the power system networks. Data tampering attacks include false data injection attacks and can seriously affect the NCSs [23]–[27]. Cyberattacks on cooperative NCSs have been studied in recent years [28], [29]. Additionally, delay-based attacks [30]–[32] and denial-of-service (DoS) attacks [33], [34] against the NCSs have been also discussed. These attacks can cause performance degradation and system destabilization, which can cause the system to halt.

In general, the confidentiality, integrity, and availability of information systems are emphasized in this order. However, in control systems, availability is the most important since a system halt causes negative effects on safety and economy. The physical and economic impacts of cyberattacks on power systems have been discussed [35]–[38]. Thus, it is necessary to maintain the operation of control systems, even if the systems are under attack [39], [40]. To maintain normal operation during a cyberattack, methods to detect data tampering attacks with predicted values [41], [42] and to mitigate data tampering attacks by switching multiple controllers [43] have been proposed. Muniraj et al. [44] proposed a detection and mitigation method for actuator attacks in motion control systems. A fallback control system is one of the approaches to achieve the minimally required operation when a motion control system is attacked [45].

For the detection and mitigation of data tampering attacks to improve the availability in networked motion control systems, in which a motor is remotely controlled over the networks, a method that applies redundant network paths has been proposed. The tamper detection observer (TDO) was proposed to detect and mitigate the data tampering attacks against the feedback network path [46]–[49]. This is the path laid from the motor side to the controller side in networked motion control systems. The TDO considers the tampered signals as a disturbance, detects the attacked path by comparing the output of a local motor model and the output of the actual motor, and mitigates the attacks by selecting the path that was not attacked from the redundant feedback network paths. However, the TDO cannot mitigate the data tampering attacks against the forward network path. This is because it changes the feedback paths that are based on the information from the feedback signals alone.

To address the issue of TDO, Yamada *et al.* [50] proposed a fixed redundant path selection (FRPS) method to detect and mitigate the data tampering attacks against the forward network path in networked motion control systems. The FRPS uses the redundant forward network paths and selects the path that is not attacked based on the majority decision. The conventional FRPS method assumes that only one path is attacked, and it does not consider simultaneous attacks against multiple paths. Increasing the number of redundant paths improves the detection performance of simultaneous attacks against multiple paths. However, it also increases the amount of traffic because the same data are transmitted to all the redundant paths. Therefore, a novel provisioning and selection method is required for the redundant network paths in order to dynamically balance the detection performance and the amount of traffic.

This study proposes a dynamic redundant path selection (DRPS) method to reduce the amount of traffic. This is achieved by changing the number of forward paths that are used in the tampering detection while addressing the simultaneous attacks against multiple redundant paths. This study focuses on the attacks against only the forward paths because the attacks against the feedback paths can be detected by the TDO, as previously discussed in [46]. In addition, the DRPS for the forward paths can be applied to not only closed-loop systems, but also open-loop systems, and has more use cases. We previously presented the DRPS concept in [51]. However, in [51], the path provisioning and selection algorithm was limited to a use case and no experimental verification was performed. Herein, the operational sequence and algorithm of the DRPS are clarified, and the experimental results are presented. The experiments confirm that the proposed DRPS outperforms the conventional FRPS.

Our main contribution lies in demonstrating that the DRPS can detect and mitigate the data tampering attacks while reducing the number of network paths that are used in tampering detection when the system is exposed to simultaneous attacks on up to two network paths. In this study, only data tampering attacks are considered. However, the proposed method may be applied to various network-based cyberattacks such as man-in-the-middle (MITM)-type attacks and network-induced faults such as network disconnection since anomaly detection is achieved by transmitting the same data on multiple network paths.

The remainder of this paper is organized as follows. The following section describes the configuration of the networked motion control system and its time-delay compensation technique. Section III describes the conventional FRPS to detect and mitigate data tampering attacks. The proposed DRPS, which reduces the number of network paths used in the tampering detection, is described in section IV. Section V presents the experimental results to confirm the effectiveness of the proposed DRPS. Finally, section VI concludes the paper.

II. NCS

This section describes the networked motion control system with a time delay. Additionally, the disturbance observer (DOB) for the robust motion control and the adaptive Smith predictor (ASP) for the time-delay compensation are discussed.

A. NETWORKED MOTION CONTROL

The block diagram of a networked angle control system for a direct current (DC) motor, including the DOB and ASP, is shown in Fig. 1. The configurations of the DOB and ASP

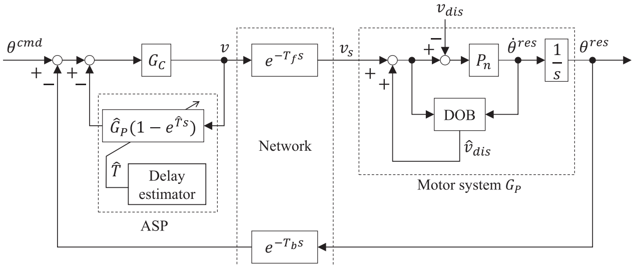


FIGURE 1. Networked motion control system.

are described in detail in sections II-B and II-C, respectively. In Fig. 1, θ^{cmd}, v, v_{dis}, $\hat{v}_{dis}$, θ^{res}, $\dot{\theta}^{res}$, T_f, and T_b denote the angle command, voltage input, disturbance in the voltage, estimated disturbance, angle response, angular velocity response, transmission delay on the forward path, and transmission delay on the feedback path, respectively. The system includes a proportional-derivative (PD) controller G_C, the actual motor system G_p, and the nominal model of the motor system P_n, which is described as (1)

$$P_n = \frac{K_n}{\tau_n s}, \tag{1}$$

where K_n, τ_n, and s denote the nominal steady-state gain of the motor, the nominal time constant of the motor, and the Laplace operator, respectively. The controller and motor system are connected through the networks. The networks are configured based on Internet protocol (IP)-based digital communication; signal errors on the network paths other than the data tampering attacks are not considered in this study. The quantization errors in an analog-digital converter are negligibly small, and additional data quantization errors are not generated for data transmission. The transfer function of the PD controller G_C is expressed as (2)

$$G_C = \frac{\tau_n}{K_n}(K_p + K_d s), \tag{2}$$

where K_p and K_d denote the proportional gain and derivative gain, respectively. In this study, we applied the DOB to achieve robust motion control against the disturbance v_{dis} [52].

B. DOB

The block diagram of the DOB is shown in Fig. 2. The DOB is implemented on the motor side. The voltage input v_s is the value received from the controller side through the network path. In Fig. 2, P is the transfer function of the actual motor system as shown in (3)

$$P = \frac{K}{\tau s + 1}, \tag{3}$$

where K and τ denote the actual steady-state gain and the time constant of the motor, respectively. The motion control system includes the modeling error between P and P_n. Additionally, the load torque is exerted on the motor as v_{load} in the dimension of voltage. These uncertainties can be considered as the disturbance v_{dis}, which is compensated by the DOB. The DOB calculates the estimated disturbance $\hat{v}^{dis}$ as (4)

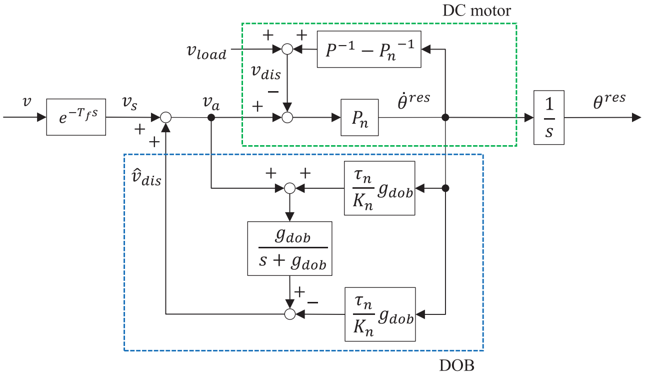


FIGURE 2. Motor system with the DOB.

$$\hat{v}_{dis} = \frac{g_{dob}}{s + g_{dob}} v_{dis}, \tag{4}$$

where g_{dob} denotes the cut-off frequency of the low-pass filter (LPF). By implementing the DOB, it can be considered that the disturbance v^{dis} is input into the system through the high-pass filter (HPF) whose cut-off frequency is g_{dob}. If the cut-off frequency g_{dob} is sufficiently large, the DOB completely suppresses the disturbance, which results in robust motion control.

C. ASP

In this study, the ASP [53] is employed as a time-delay compensator. The ASP can compensate for a time-varying delay differently from the classical Smith predictor (SP) [54], which compensates for only a constant time delay. This is because the ASP updates the delay model by measuring the round-trip time (RTT) between the controller and the motor sides. This study assumes that the transmission delay on each network path is constant. In the FRPS and DRPS, however, the time delay in the closed loop changes depending on the selected path. Since the RTT model in the time-delay compensator must be updated, this study adopts the ASP rather than the classical SP. This study does not consider packet losses. If there are frequent packet losses on a network path, another compensation technique such as a communication disturbance observer (CDOB) [55] may be necessary.

The RTT in the control system, T, is defined as (5)

$$T = T_f + T_b. \tag{5}$$

In the ASP shown in Fig. 1, $\hat{G}_p$ and $\hat{T}$ denote the nominal motor system including the DOB and the RTT measured by the delay estimator, respectively. If the ASP is not implemented, the transfer function from θ^{cmd} to θ^{res} is given by (6)

$$\frac{\theta^{res}}{\theta^{cmd}} = \frac{G_C G_P e^{-T_f s}}{1 + G_C G_P e^{-Ts}}. \tag{6}$$

In (6), since the delay element exists in the denominator of the transfer function, the controller must be designed considering the transmission delays with respect to the system stability.

If the ASP is implemented, the transfer function from θ^{cmd} to θ^{res} is given by (7)

$$\frac{\theta^{res}}{\theta^{cmd}} = \frac{G_C G_P e^{-T_f s}}{1 + G_C \hat{G}_P + G_C \hat{G}_P e^{-\hat{T}s} - G_C G_P e^{-Ts}}. \quad (7)$$

The delay estimator measures the RTT between the controller and the motor sides with the timestamp information from the exchanged packets and updates the RTT model, which results in $T = \hat{T}$. If the cut-off frequency of the DOB is infinity, $G_P = \hat{G}_P$ is satisfied. Therefore, (7) can be transformed into (8)

$$\frac{\theta^{res}}{\theta^{cmd}} = \frac{G_C G_P e^{-T_f s}}{1 + G_C G_P}. \quad (8)$$

The delay element is eliminated from the denominator of the transfer function, or equivalently, the transmission time delays are not included in the feedback loop. As a result, this simplifies the feedback controller design.

III. FRPS

This section describes the conventional detection and mitigation method of data tampering attacks using the FRPS. The FRPS has no path provisioning functions, and it uses a constant number of redundant network paths in the tampering detection.

A. SYSTEM CONFIGURATION

The block diagram of the networked motion control system with the FRPS is shown in Fig. 3. The PD controller and ASP are implemented on the controller side, and the DOB is implemented on the motor side. In this system, n forward network paths are set to detect and mitigate up to $(n-1)/2$ simultaneous attacks against the forward network paths. It is noted that n is an arbitrary odd integer used to find an attacked path based on a majority decision. The controller transmits the voltage input v for all of the redundant paths. The redundant network paths should be configured using different communication interfaces, such as wired Ethernet, Wi-Fi, or 5G, to enhance security even at the expense of cost. If a wireless communication interface with different frequencies is utilized for the redundant network paths, each network path may be affected by inter-channel interference, resulting in quality-of-service (QoS) degradation through problems such as time-varying delays.

Herein, the data tampering attacks are modeled as additive disturbances as $f_1, f_2, \cdots$, and f_n for each forward network path. Additionally, each forward network path has a transmission delay expressed as $T_1, T_2, \cdots$, and T_n. The assumption that the delays take constant values is reasonable because a time-varying delay can be transformed into a constant delay by using a jitter buffer on the receiver side [56]. Note that the regulated delay equals the maximum value of the transmission delays on a path if the jitter buffer is installed. The path selector is installed on the motor side to receive all the delayed voltage inputs as $v_1, v_2, \cdots$, and v_n. Then, the path selector selects the voltage input v_s of a path that is not attacked. This is decided based on the majority decision. The ASP is used to compensate for the effect of the transmission delay, which varies depending on the selected forward network path.

B. PATH SELECTOR ALGORITHM

The operation of the path selector with the FRPS is shown in Fig. 4, where $v_{k,t}$ and $v_{s,t}$ denote the delayed voltage input that is received by the path selector from path k at time t and the selected voltage input at time t, respectively. The time t is updated in every control period st. Each forward network path has a different transmission delay. The path number k is assigned in ascending order of the delay, i.e., path 1 has the smallest transmission delay and path n has the largest transmission delay. In this study, it is assumed that the transmission delay of each path is constant and the path selector has the information of each delay.

First, the number of forward network paths, n, is set. The number n is determined according to the assumed number of simultaneous attacks. The path selector waits to receive the delayed voltage inputs $v_{k,t}$ from all n redundant paths. If the path selector does not have all n delayed voltage inputs at time t, the path selector outputs the same value as $v_{s,t-st}$, which is the selected voltage output in the previous control period. Otherwise, the path selector obtains the delay-adjusted voltage inputs $v'_{k,t}$ from the receiving buffer. The relationship between $v_{k,t}$ and $v'_{k,t}$ is shown in (9)

$$v'_{k,t} = v_{k,t-(T_{max}-T_k)}, \quad (9)$$

where T_{max} denotes the largest transmission delay of the n paths. This should ideally result in the same value for all of $v'_{k,t}$ at time t if no network paths are attacked.

Then, the path selector determines the selected voltage input $v_{s,t}$ as shown in Algorithm 1. The attacks that are against a part of the forward network paths can result in different delay-adjusted voltage inputs $v'_{k,t}$ at time t. Therefore, the path that is not attacked can be determined based on the majority decision provided that the number of attacked paths is less than $(n+1)/2$. The path selector chooses the path with the smallest transmission delay among all paths that are not attacked. These processes are repeated until the end time t_{end} in every control period st.

When the NCS does not have a path selector, it can utilize the voltage input with the minimum transmission delay while not detecting the attacks. In contrast, when the NCS has a path selector, it can detect the attacks while utilizing the voltage input with the maximum transmission delay. Therefore, the path selector detects the attacks at the expense of control performance, which can be deteriorated through a large transmission delay. The ASP is thus implemented to mitigate the performance deterioration as much as possible.

IV. DRPS

This section describes the proposed detection and mitigation method of data tampering attacks using the DRPS.

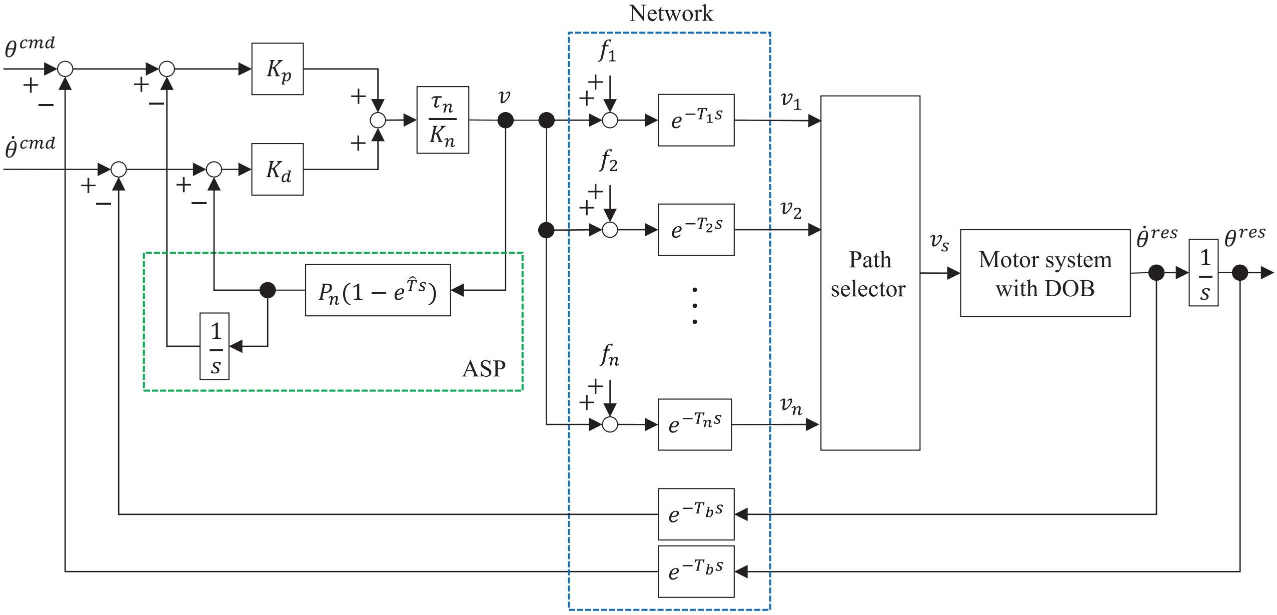


FIGURE 3. Configuration of the system that employs FRPS.

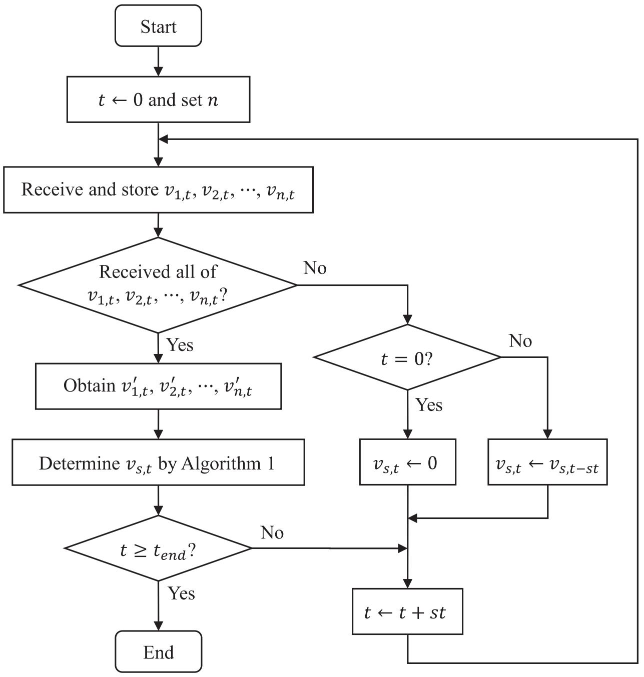

Start
$t \leftarrow 0$ and set n
Receive and store $v_{1,t}, v_{2,t}, \cdots, v_{n,t}$
Received all of $v_{1,t}, v_{2,t}, \cdots, v_{n,t}$?
No
Yes
$t = 0$?
No
Yes
Obtain $v'_{1,t}, v'_{2,t}, \cdots, v'_{n,t}$
Determine $v_{s,t}$ by Algorithm 1
$v_{s,t} \leftarrow 0$
$v_{s,t} \leftarrow v_{s,t-st}$
$t \geq t_{end}$?
No
Yes
$t \leftarrow t + st$
End

FIGURE 4. Operation of the path selector with the FRPS.

Algorithm 1 Determination of $v_{s,t}$ in the FRPS

```
for $k \leftarrow 1$ to $n$ do
    $d_{cnt} \leftarrow 0$
    for $i \leftarrow 1$ to $n$ do
        if $|v'_{i,t} - v'_{k,t}| > 0$ then
            $d_{cnt} \leftarrow d_{cnt} + 1$
        end if
    end for
    if $d_{cnt} < \frac{n+1}{2}$ then
        $v_{s,t} \leftarrow v'_{k,t}$
        break
    else
        $v_{s,t} \leftarrow v_{s,t-st}$
    end if
end for
```

The DRPS has a network provisioning function and it dynamically changes the number of redundant network paths that are used in the tampering detection to reduce the amount of traffic.

A. SYSTEM CONFIGURATION

The block diagram of the networked motion control system with the DRPS is shown in Fig. 5. The PD controller and ASP are implemented on the controller side, and the DOB is implemented on the motor side, as is the case with the FRPS. In this system, m candidate paths can be employed, whereas n paths of the m candidate paths are set during the path provisioning to detect and mitigate up to $(n-1)/2$ simultaneous attacks against the forward network paths. It is noted that n is a dynamic odd integer, e.g., three or five in this study, used to find attacked paths based on the majority decision. The controller transmits the voltage input v for all of the n redundant paths. The DRPS can reduce the amount of traffic by changing the number of forward network paths that are used in the tampering detection while addressing the simultaneous attacks against up to two of the redundant paths.

In this study, the data tampering attacks are modeled as additive disturbances as $f_1, f_2, \cdots$, and f_m for each forward

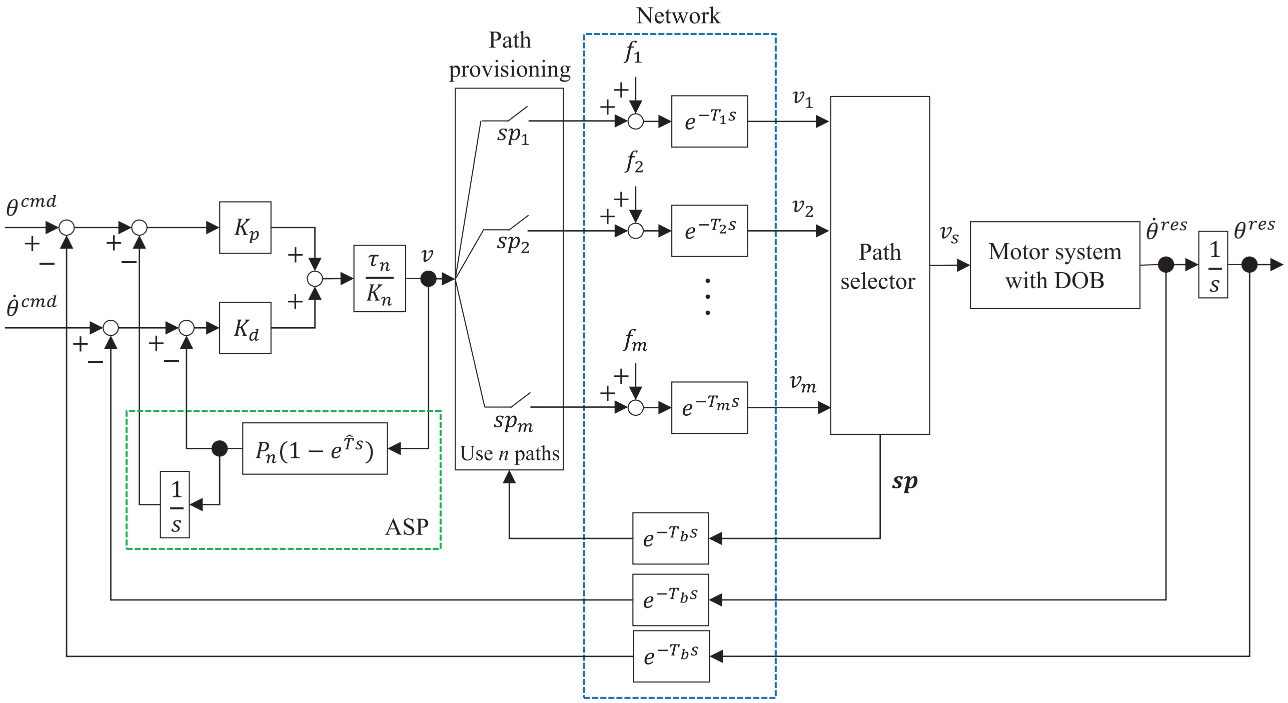


FIGURE 5. Configuration of the system that employs the DRPS.

network path. It is assumed that the attacked paths can be changed at intervals much longer than an RTT, and that an attack continues for at least an RTT. Additionally, each forward network path has a transmission delay expressed as $T_1, T_2, \cdots$, and T_m. The path selector is installed on the motor side to receive all the delayed voltage inputs as v_1, $v_2, \cdots$, and v_m. Furthermore, it selects the voltage input v_s of a path that is not attacked based on the majority decision. The ASP is used to compensate for the effect of the transmission delay.

The path selector also outputs the m-dimensional switching vector $\boldsymbol{sp}$. The path provisioning function on the controller side receives the information of $\boldsymbol{sp}$, extracts the elements of the vectors sp_1, $sp_2, \cdots$, and sp_m, and changes the paths that are used. If path k is used for the detection, the k-th element of $\boldsymbol{sp}$ is set to 1 and the voltage input v is transmitted through path k from the controller side. Otherwise, the k-th element of $\boldsymbol{sp}$ is set to 0 and the voltage input v is not transmitted through path k from the controller side. The vector $\boldsymbol{sp}$ is transmitted to the controller side through the feedback path with the transmission delay T_b. The transmission of the switching vector $\boldsymbol{sp}$ does not have a negative impact on the amount of traffic compared to the FRPS, since the position, velocity, and switching vector can be included in a minimum-size Ethernet frame. The attacks against the feedback path may destabilize the system, as is the case with the FRPS. The TDO can be additionally implemented to obtain reliable feedback signals.

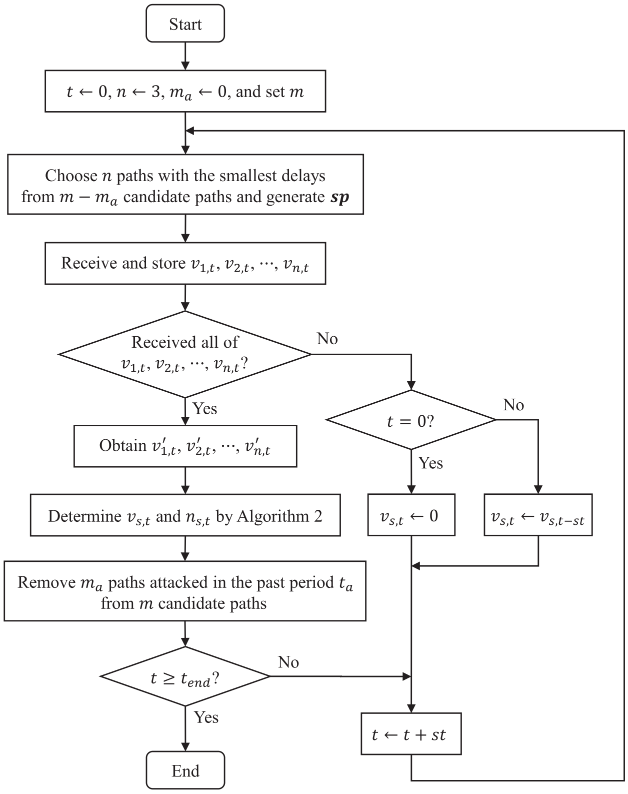

Start
$t \leftarrow 0$, $n \leftarrow 3$, $m_a \leftarrow 0$, and set m
Choose n paths with the smallest delays from $m - m_a$ candidate paths and generate $\boldsymbol{sp}$
Receive and store $v_{1,t}$, $v_{2,t}$, $\cdots$, $v_{n,t}$
Received all of $v_{1,t}$, $v_{2,t}$, $\cdots$, $v_{n,t}$?
No
Yes
$t = 0$?
No
Yes
Obtain $v'_{1,t}$, $v'_{2,t}$, $\cdots$, $v'_{n,t}$
Determine $v_{s,t}$ and $n_{s,t}$ by Algorithm 2
$v_{s,t} \leftarrow 0$
$v_{s,t} \leftarrow v_{s,t-st}$
Remove m_a paths attacked in the past period t_a from m candidate paths
$t \geq t_{end}$?
No
Yes
$t \leftarrow t + st$
End

FIGURE 6. Operation of the path selector with the DRPS.

B. PATH SELECTOR ALGORITHM

The operation of the path selector with the DRPS is shown in Fig. 6. The parameter m is newly introduced in the DRPS to operate the system while removing the recently attacked paths during the period t_a after the attacks are detected. The number of attacked paths in the past period t_a is defined as m_a. Therefore, $m - m_a$ paths can be used for the detection and mitigation of the attacks. The parameter m can be set under the condition of $m \geq (3n_{max} - 1)/2$, where n_{max} denotes the maximum value of n. It is assumed that changes in the attacked paths do not occur frequently, i.e., with a period of less than t_a. The variables $v_{k,t}$ and $v'_{k,t}$ are defined for the n paths that are used for the detection, as demonstrated with the FRPS. The path number k is assigned in the ascending order of the delay. Additionally, we assumed that the transmission delay of each path is constant, and the path selector has the information for each delay.

First, the number of candidate paths m is set. In the initial condition, n and m_a are set to three and zero, respectively. Unlike the FRPS, n paths with the smallest delays are chosen from the $m - m_a$ candidate paths. The path selector generates the switching vector $\boldsymbol{sp}$ to inform the paths that are to be used for the detection of the controller side. The path selector waits to receive the delayed voltage inputs $v_{k,t}$ from all of the n redundant paths. If the path selector does not have all of the n delayed voltage inputs at time t, the path selector outputs the same value as $v_{s,t-st}$, which is the selected voltage output in the previous control period. Otherwise, the path selector obtains the delay-adjusted voltage inputs $v'_{k,t}$ from a receiving buffer as (9). This should ideally result in the same value for all of $v'_{k,t}$ at time t if none of the network paths are attacked.

Then, the path selector determines the selected voltage input $v_{s,t}$ and the number of paths to be provisioned at time t, $n_{s,t}$, which can be either three or five, as shown in Algorithm 2. When the delay-adjusted voltage inputs of all n paths are the same, $n_{s,t}$ is set to three only if $n = n_{s,t-st} = 3$ or $n = 5$. Unlike Algorithm 1, the path selector checks the presence or absence of attacks when $n = 3$. If at least one of the three delay-adjusted voltage inputs is different from the others, it is believed that there are attacks that are being performed against one or two paths. Therefore, the path selector increases $n_{s,t}$ from three to five, it determines the path that is not attacked based on the majority decision, and it removes m_a paths that were attacked in the past period t_a from the m candidate paths. Note that $v_{s,t-st}$ is utilized instead of $v_{s,t}$ when the path provisioning to increase the number of used paths is not completed, because $v_{s,t}$ may be attacked. The duration of the path provisioning is at least an RTT, and this delay may affect the detection performance differently from the case of the FRPS. The path selector chooses the path with the smallest transmission delay among all the paths that are not attacked. These processes are repeated until the end time t_{end} in every control period st.

V. EXPERIMENT

This section presents the experimental results to confirm the effectiveness of the proposed method.

A. SETUP

The experiments of the remote angle control were performed using a DC servo motor. The experimental setup is shown in Fig. 7. The network delays were virtually inserted in the controller using LabVIEW. The parameters that were used in the experiments are shown in Table 1. All methods compared in the experiments utilized the same control parameters: K_p, K_d, and g_{dob}. The proportional and derivative gains of the PD controller, K_p and K_d, respectively, were set to satisfy the condition for critical damping. The cut-off frequency of the DOB, g_{dob}, was experimentally determined considering system noise.

The following three methods are compared in terms of tracking, the performance of the tamper detection, and the amount of traffic under the data tampering attacks. One method is the conventional FRPS that has $n = 3$, which is defined as FRPS-3. Another is the conventional FRPS where $n = 5$, which is defined as FRPS-5. The third is the proposed DRPS where $m = 7$ and $n_{max} = 5$. The experiments were conducted with two types of data tampering

Algorithm 2 Determination of $v_{s,t}$ and $n_{s,t}$ in the DRPS

```
for $k \leftarrow 1$ to $n$ do
    $d_{cnt} \leftarrow 0$
    for $i \leftarrow 1$ to $n$ do
        if $|v'_{i,t} - v'_{k,t}| > 0$ then
            $d_{cnt} \leftarrow d_{cnt} + 1$
        end if
    end for
    if $d_{cnt} = 0$ and ($n = n_{s,t-st} = 3$ or $n = 5$) then
        $v_{s,t} \leftarrow v'_{k,t}$
        $n_{s,t} \leftarrow 3$
        break
    else if $n = 3$ then
        $v_{s,t} \leftarrow v_{s,t-st}$
        $n_{s,t} \leftarrow 5$
        break
    else if $d_{cnt} < 3$ and $n = 5$ then
        $v_{s,t} \leftarrow v'_{k,t}$
        $n_{s,t} \leftarrow 5$
        break
    else
        $v_{s,t} \leftarrow v_{s,t-st}$
    end if
end for
```

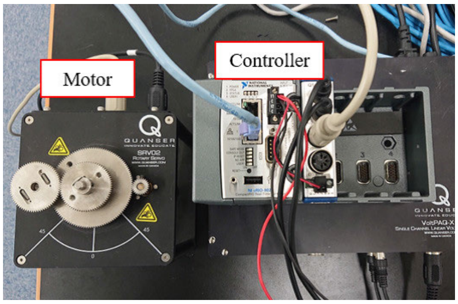


FIGURE 7. Experimental setup.

TABLE 1. Parameters that were used in the experiments.

Nominal steady-state gain of the motor	K_n	0.153
Nominal time constant of the motor	τ_n	0.00254
Proportional gain	K_p	225
Derivative gain	K_d	30
Cut-off frequency of the DOB	g_{dob}	100 rad/s
Transmission delay on the feedback path	T_b	10 ms
Control period	st	1 ms
Removal time for the attacked paths	t_a	6 s
Transmission delay of forward path 1	T_1	10 ms
Transmission delay of forward path 2	T_2	20 ms
Transmission delay of forward path 3	T_3	30 ms
Transmission delay of forward path 4	T_4	40 ms
Transmission delay of forward path 5	T_5	50 ms
Transmission delay of forward path 6	T_6	60 ms
Transmission delay of forward path 7	T_7	70 ms

TABLE 2. Type A data tampering attacks.

	$0\,\mathrm{s} \leqq t < 1\,\mathrm{s}$	$1\,\mathrm{s} \leqq t < 2\,\mathrm{s}$	$2\,\mathrm{s} \leqq t \leqq 3\,\mathrm{s}$
f_1	0	$5\sin(20\pi t)$	0
f_2	0	0	0
f_3–f_7	0	0	0

TABLE 3. Type B data tampering attacks.

	$0\,\mathrm{s} \leqq t < 1\,\mathrm{s}$	$1\,\mathrm{s} \leqq t < 2\,\mathrm{s}$	$2\,\mathrm{s} \leqq t \leqq 3\,\mathrm{s}$
f_1	0	$5\sin(20\pi t)$	0
f_2	0	$5\sin(20\pi t)$	0
f_3–f_7	0	0	0

attacks, i.e., types A and B, as shown in Table 2 and 3, respectively. Type A indicates the attacks that are against one of the forward network paths, and type B indicates the simultaneous attacks against two forward network paths. In the experiments, the computation time of the controller and path selector algorithms in all methods at each sampling time was within the control period. Increasing the number of network paths used and the degrees of freedom of the mechanical system may result in a longer computation time. Our future work will include the enhancement of scalability to address this issue.

B. RESULTS

The experimental results of each method with the data tampering attacks of type A are shown in Figs. 8–10, which indicate the tracking performance, selected path number, and number of paths used in the tampering detection, respectively. The experimental results of each method with the data tampering attacks of type B are shown in Figs. 11–13, which indicate the tracking performance, selected path number, and number of paths used in the tampering detection, respectively.

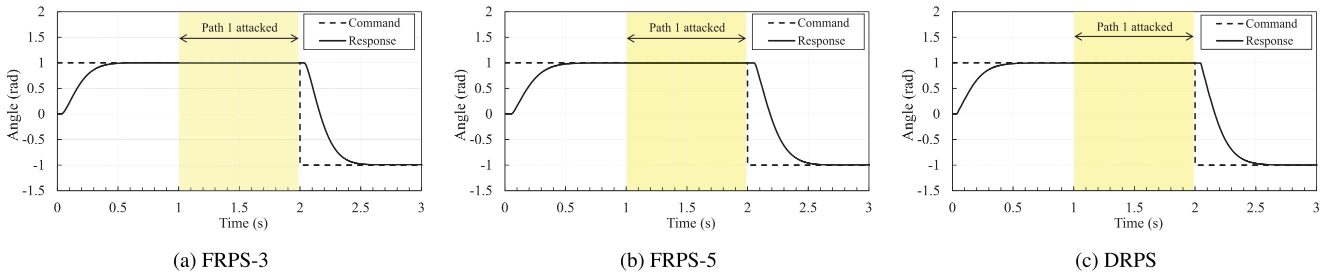
In Fig. 8, all methods achieved angle control by mitigating the attacks. FRPS-3 and DRPS started tracking the command at 30 ms, and FRPS-5 started tracking the command at 50 ms. These results come from the difference in the maximum delay of the paths that are used in the tampering detection. At first, FRPS-3 and DRPS utilized three paths, i.e., paths 1, 2, and 3. Since the maximum delay of the three paths was 30 ms for path 3, the angle responses rose at approximately 30 ms. In contrast, FRPS-5 utilized five paths, i.e., paths 1, 2, 3, 4, and 5. Since the maximum delay of the five paths was 50 ms for path 5, the angle response rose at approximately 50 ms. After the attacks for path 1 had ended at 2 s, FRPS-3, FRPS-5, and DRPS started tracking the command at 2.03 s, 2.05 s, and 2.04 s, respectively. This is because the DRPS removed the attacked path and utilized paths 2, 3, and 4 for the tampering detection. The response delay changed in the DRPS because the maximum delay of the three paths changed from 30 ms to 40 ms.

In Fig. 9, all methods indicated that path 1 was attacked, and the selected path was changed from path 1 to path 2 after the attacks had been inserted. Only the DRPS continued selecting path 2 after the attacks had stopped, as the attacked path was removed from the candidate paths during t_a. FRPS-3 and FRPS-5 detected the attacks and changed the selected paths at 1.03 s and 1.05 s, respectively. In contrast, the DRPS started avoiding the effect of the attacks at 1.03 s and completed the change of the selected path at 1.09 s. This is because the DRPS needs additional control signals to be exchanged between the controller and the motor sides to change the paths that are used in the tampering detection.

In Fig. 10, FRPS-3 and FRPS-5 utilized three and five paths, respectively, for the tampering detection, and the DPRS dynamically changed the number of used paths. Additionally, the DRPS changed the number of used paths multiple times when the attacks were inserted. This is because the switching vector could not be set instantly owing to the transmission delays, and the condition $d_{cnt} = 0$ had been satisfied before the switching vector was received on the controller side. For the type A attacks, FRPS-3 and DRPS provided better performance than FRPS-5 with respect to the amount of traffic since they used fewer paths for the tampering detection while maintaining the tracking performance. Furthermore, it was confirmed that DRPS exhibited the slowest response after the tampering detection because the switching vector must have been transmitted.

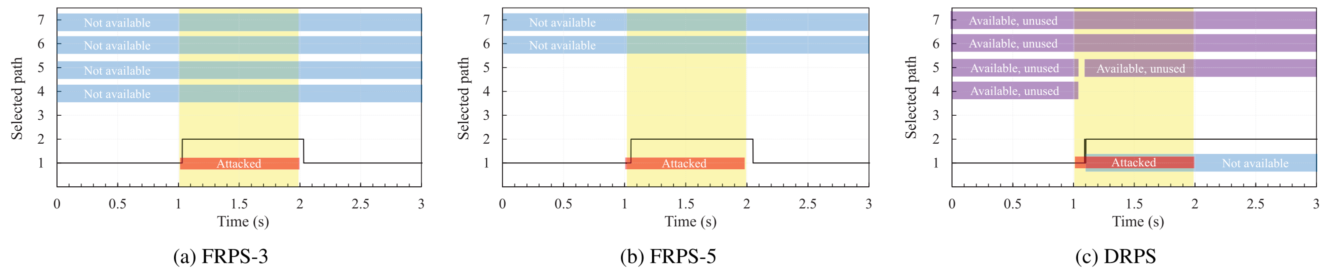
In Fig. 11, FRPS-5 and DRPS achieved angle control by mitigating the attacks, whereas FRPS-3 was greatly affected by the attacks. FRPS-3 could not detect the simultaneous attacks against the two forward network paths by the majority decision since the number of used paths was only three. After the attacks for paths 1 and 2 had ended at 2 s, FRPS-3, FRPS-5, and DRPS started tracking the command at 2.03 s, 2.05 s, and 2.05 s, respectively. This is because the DRPS removed the attacked paths and utilized paths 3, 4, and 5 for the tampering detection. The response delay changed in the DRPS because the maximum delay of the three paths changed from 30 ms to 50 ms.

In Fig. 12, FRPS-5 and DRPS determined that paths 1 and 2 were attacked and changed the selected paths from path 1 to path 3 after the attacks had been inserted. Only the DRPS continued selecting path 3 after the attacks had stopped, as the attacked paths were removed from the candidate paths dur-



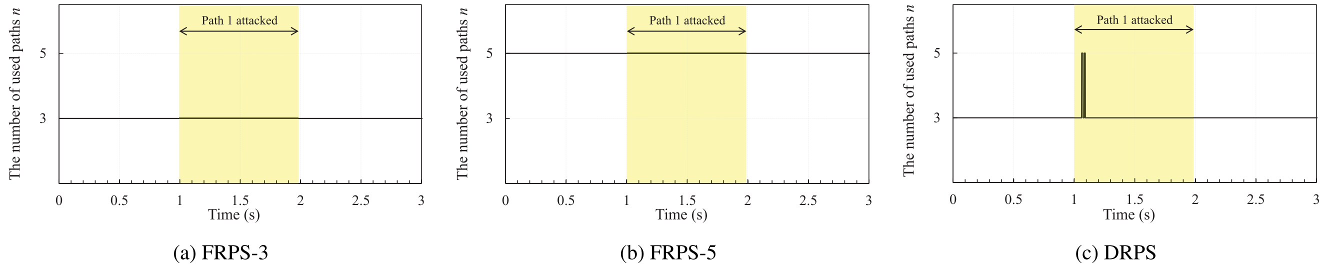
(a) FRPS-3 (b) FRPS-5 (c) DRPS

FIGURE 8. Tracking performance for the type A attacks.



(a) FRPS-3 (b) FRPS-5 (c) DRPS

FIGURE 9. Selected path number for the type A attacks.



(a) FRPS-3 (b) FRPS-5 (c) DRPS

FIGURE 10. Number of paths used in the tampering detection for the type A attacks.

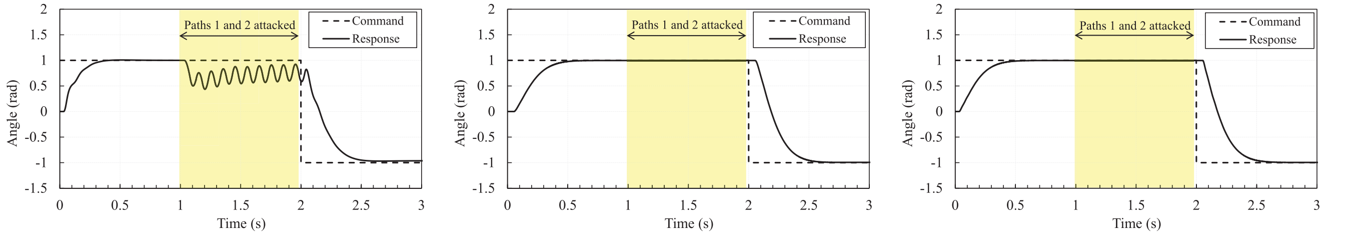
ing t_a. FRPS-5 detected the attacks and changed the selected paths at 1.05 s. In contrast, the DRPS started avoiding the effect of the attacks at 1.03 s and completed the change in the selected path at 1.09 s.

In Fig. 13, FRPS-3 and FRPS-5 always used three and five paths for the tampering detection, and DPRS dynamically changed the number of used paths. DRPS increased the number of used paths from three to five at the start of the tampering detection and decreased the number of used paths from five to three immediately after the tampering detection. Although the transmission of the switching vector generated an additional delay in the DRPS, the system was not affected by the attacks, as the path selector continued to input the voltage value stored before the tampering detection to the motor system. For the type B attacks, the DRPS provided better performance than any of the other methods in terms of the amount of traffic and the tracking performance.

VI. CONCLUSION

This study proposed the DRPS as a network path provisioning and selection method to reduce the amount of traffic during the tampering detection. The DRPS changed the number of forward paths used in the tampering detection while mitigating simultaneous attacks against multiple paths. The experimental results demonstrated that the proposed DRPS outperformed the conventional FRPS since the DRPS could detect and mitigate the data tampering attacks while reducing the number of paths used when the system was exposed to simultaneous attacks on up to two redundant paths.

Herein, we assumed that the simultaneous attacks were against up to two network paths. This assumption was made because the redundant paths should be designed such that they have different communication interfaces and simultaneous attacks against three or more paths have low potential. Note that the proposed DRPS has scalability to deal with the detection and mitigation of any number of simultaneous attacks

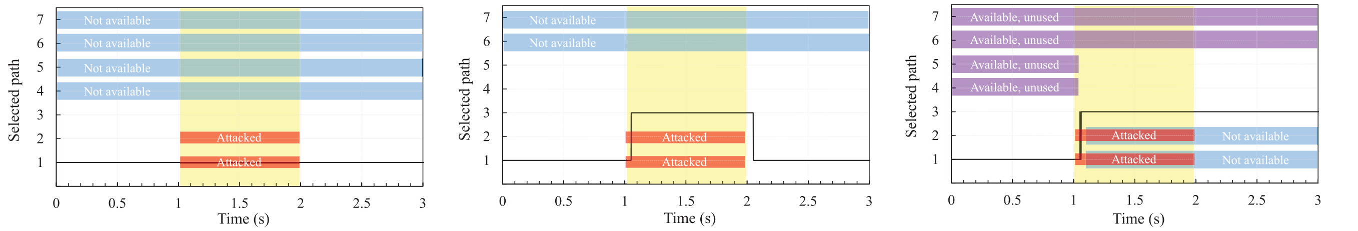


(a) FRPS-3

(b) FRPS-5

(c) DRPS

FIGURE 11. Tracking performance for the type B attacks.

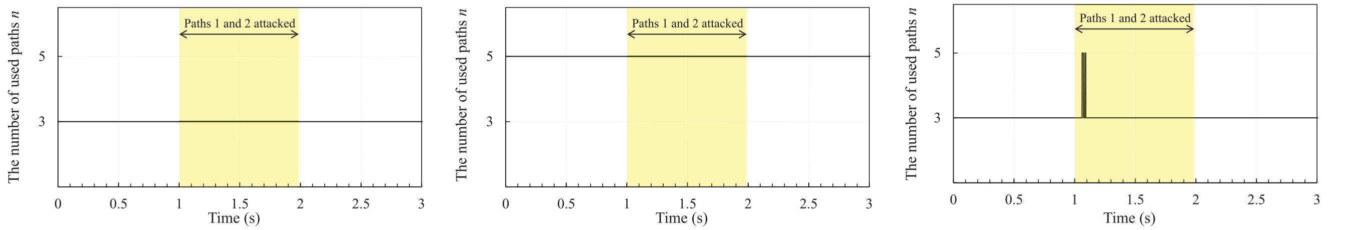


(a) FRPS-3

(b) FRPS-5

(c) DRPS

FIGURE 12. Selected path number for the type B attacks.



(a) FRPS-3

(b) FRPS-5

(c) DRPS

FIGURE 13. Number of paths used in the tampering detection for the type B attacks.

against the network paths. Applying duplicated routes should be avoided because this approach has a significantly greater chance of being vulnerable to simultaneous attacks against some paths. However,the problem remains that installing different communication interfaces increases capital expenditure. In addition, the DRPS cannot mitigate attacks with durations shorter than an RTT owing to the transmission delays. To address this type of attack, an additional mitigation technique is necessary.

Our future research will include the development of a path provisioning mechanism to address any number of simultaneous attacks. This is performed in combination with a mechanism to periodically increase the number of network paths that are applied during the tampering detection. Moreover, the combination of the proposed DRPS for the forward paths and the conventional TDO for the feedback paths requires further study concerning the synchronization of path switching. Since the TDO includes the model of the motor system, it may detect not only cyberattacks but also sensor faults. However, how to stop the operation or switch to a fallback operation after the detection is an open issue. The expansion of our proposed DRPS into more general systems is also considered. For example, future work could verify the DRPS in open-loop systems and devise a method for coping with signal noise on the network paths. As for the signal noise, the introduction of clustering algorithms into the path selector is one possible solution. The proposed method cannot detect direct attacks on servers and systems such as DoS attacks, and has to be combined with a network control technique or observer-based method.

REFERENCES

[1] F.-L. Lian, J. R. Moyne, and D. M. Tilbury, "Performance evaluation of control networks: Ethernet, ControlNet, and DeviceNet," *IEEE Control Syst.*, vol. 21, no. 1, pp. 66–83, Feb. 2001.

[2] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE Trans. Ind. Electron.*, vol. 57, no. 7, pp. 2527–2535, Jul. 2010.

[3] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th Design Automat. Conf. (DAC)*, Jun. 2010, pp. 731–736.

[4] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[5] A. P. Batista and F. G. Jota, "Performance improvement of an NCS closed over the internet with an adaptive Smith predictor," *Control Eng. Pract.*, vol. 71, pp. 34–43, Feb. 2018.

[6] M. Hamdy, S. Abd-Elhaleem, and M. A. Fkirin, "Time-varying delay compensation for a class of nonlinear control systems over network via H_∞ adaptive fuzzy controller," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 8, pp. 2114–2124, Aug. 2017.

[7] M. Hamdy, S. Abd-Elhaleem, and M. A. Fkirin, "Adaptive fuzzy predictive controller for a class of networked nonlinear systems with time-varying delay," *IEEE Trans. Fuzzy Syst.*, vol. 26, no. 4, pp. 2135–2144, Aug. 2018.

[8] M. Hamdy, S. Abd-Elhaleem, and M. A. Fkirin, "Design of adaptive fuzzy control for a class of networked nonlinear systems," *J. Dyn. Syst., Meas., Control*, vol. 139, no. 3, pp. 031008-1–031008-9, Mar. 2017.

[9] X. Sun and X. Meng, "A robust control approach to event-triggered networked control systems with time-varying delays," *IEEE Access*, vol. 9, pp. 64653–64664, 2021.

[10] Y. Lei, Y. Yuan, and J. Zhao, "Model-based detection and monitoring of the intermittent connections for CAN networks," *IEEE Trans. Ind. Electron.*, vol. 61, no. 6, pp. 2912–2921, Jun. 2014.

[11] A. M. H. Teixeira, J. Araújo, H. Sandberg, and K. H. Johansson, "Distributed sensor and actuator reconfiguration for fault-tolerant networked control systems," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 4, pp. 1517–1528, Dec. 2018.

[12] A. H. Tahoun, "Fault-tolerant control for a class of quantised networked control of nonlinear systems with unknown time-varying sensor faults," *Int. J. Control*, vol. 93, no. 3, pp. 619–628, Mar. 2020.

[13] E. A. Lee, "Cyber physical systems: Design challenges," in *Proc. 11th IEEE Int. Symp. Object Compon.-Oriented Real-Time Distrib. Comput. (ISORC)*, May 2008, pp. 363–369.

[14] H. Sandberg, S. Amin, and K. Johansson, "Cyberphysical security in networked control systems: An introduction to the issue," *IEEE Control Syst.*, vol. 35, no. 1, pp. 20–23, Feb. 2015.

[15] K. Paridari, N. O'Mahony, A. E.-D. Mady, R. Chabukswar, M. Boubekeur, and H. Sandberg, "A framework for attack-resilient industrial control systems: Attack detection and controller reconfiguration," *Proc. IEEE*, vol. 106, no. 1, pp. 113–128, Jan. 2018.

[16] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," in *Proc. 1st Int. Conf. High Confidence Netw. Syst. (HiCoNS)*, 2012, pp. 5–64.

[17] Q. Zhu, C. Rieger, and T. Basar, "A hierarchical security architecture for cyber-physical systems," in *Proc. 4th Int. Symp. Resilient Control Syst. (ISRCS)*, Aug. 2011, pp. 15–20.

[18] X. Jin, W. M. Haddad, and T. Yucelen, "An adaptive control architecture for mitigating sensor and actuator attacks in cyber-physical systems," *IEEE Trans. Autom. Control*, vol. 62, no. 11, pp. 6058–6064, Nov. 2017.

[19] A. Khalid, P. Kirisci, Z. H. Khan, Z. Ghrairi, K.-D. Thoben, and J. Pannek, "Security framework for industrial collaborative robotic cyber-physical systems," *Comput. Ind.*, vol. 97, pp. 132–145, May 2018.

[20] A. O. de Sá, L. F. R. da Costa Carmo, and R. C. S. Machado, "Covert attacks in cyber-physical control systems," *IEEE Trans. Ind. Informat.*, vol. 13, no. 4, pp. 1641–1651, Aug. 2017.

[21] W. Li, L. Xie, and Z. Wang, "Two-loop covert attacks against constant value control of industrial control systems," *IEEE Trans. Ind. Informat.*, vol. 15, no. 2, pp. 663–676, Feb. 2019.

[22] C. Zhou, Z. Wang, W. Huang, and Y. Guo, "Research on network security attack detection algorithm in smart grid system," in *Proc. IEEE Int. Conf. Saf. Produce Informatization (IICSPI)*, Dec. 2018, pp. 1407–1410.

[23] J. Wu, M. Yang, and C. Peng, "Event-based attack tolerant for a class of false data injection in networked control systems," in *Proc. 5th IEEE Int. Conf. Cloud Comput. Intell. Syst. (CCIS)*, Nov. 2018, pp. 152–157.

[24] B. Gerard, S. B. Rebai, H. Voos, and M. Darouach, "Cyber security and vulnerability analysis of networked control system subject to false-data injection," in *Proc. Annu. Amer. Control Conf. (ACC)*, Jun. 2018, pp. 992–997.

[25] L. Liu and Z. Xi, "False data injection attack sequence design against quantized networked control systems," in *Proc. IEEE Int. Conf. Unmanned Syst. (ICUS)*, Oct. 2019, pp. 542–547.

[26] A. Sargolzaei, K. Yazdani, A. Abbaspour, C. D. Crane, and W. E. Dixon, "Detection and mitigation of false data injection attacks in networked control systems," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4281–4292, Jun. 2020.

[27] M. Ghaderi, K. Gheitasi, and W. Lucia, "A blended active detection strategy for false data injection attacks in cyber-physical systems," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 168–176, Mar. 2021.

[28] Z. Elrewini, K. Sadatsharan, D. F. Selvaraj, S. J. Plathottam, and P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Veh. Commun.*, vol. 23, pp. 1–28, Jun. 2020.

[29] A. H. Tahoun and M. Arafa, "Cooperative control for cyber–physical multi-agent networked control systems with unknown false data-injection and replay cyber-attacks," *ISA Trans.*, vol. 110, pp. 1–14, Apr. 2021.

[30] A. Sargolzaei, K. K. Yen, M. N. Abdelghani, S. Sargolzaei, and B. Carbunar, "Resilient design of networked control systems under time delay switch attacks, application in smart grid," *IEEE Access*, vol. 5, pp. 15901–15912, 2017.

[31] X. Lou, C. Tran, R. Tan, D. Yau, and Z. Kalbarczyk, "Assessing and mitigating impact of time delay attack: A case study for power grid frequency control," in *Proc. 10th ACM/IEEE Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Apr. 2019, pp. 207–216.

[32] A. Abbasspour, A. Sargolzaei, M. Victorio, and N. Khoshavi, "A neural network-based approach for detection of time delay switch attack on networked control systems," *Proc. Comput. Sci.*, vol. 168, pp. 279–288, May 2020.

[33] N. Zhao, P. Shi, W. Xing, and J. Chambers, "Observer-based event-triggered approach for stochastic networked control systems under denial of service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 8, no. 1, pp. 158–167, Mar. 2021.

[34] Y. Wan, G. Wen, X. Yu, and T. Huang, "Distributed consensus tracking of networked agent systems under denial-of-service attacks," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 10, pp. 6183–6196, Oct. 2021.

[35] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[36] U. Tatar, H. Bahsi, and A. Gheorghe, "Impact assessment of cyber attacks: A quantification study on power generation systems," in *Proc. 11th Syst. Syst. Eng. Conf. (SoSE)*, Jun. 2016, pp. 1–6.

[37] K. Pan, D. Gusain, and P. Palensky, "Modelica-supported attack impact evaluation in cyber physical energy system," in *Proc. IEEE 19th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2019, pp. 228–233.

[38] J. Johnson, J. Quiroz, R. Concepcion, F. Wilches-Bernal, and M. J. Reno, "Power system effects and mitigation recommendations for DER cyberattacks," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 4, no. 3, pp. 240–249, Sep. 2019.

[39] A. A. Yaseen and M. Bayart, "Attack-tolerant networked control system based on the deception for the cyber-attacks," in *Proc. World Congr. Ind. Control Syst. Secur. (WCICSS)*, Dec. 2015, pp. 37–44.

[40] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[41] E. Mousavinejad, F. Yang, Q.-L. Han, and L. Vlacic, "A novel cyber attack detection method in networked control systems," *IEEE Trans. Cybern.*, vol. 48, no. 11, pp. 3254–3264, Nov. 2018.

[42] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, Sep. 2012.

[43] A. O. D. Sa, L. F. R. D. C. Carmo, and R. C. S. Machado, "Use of switching controllers for mitigation of active identification attacks in networked control systems," in *Proc. IEEE 15th Int. Conf. Dependable, Autonomic Secure Comput., 15th Int. Conf. Pervas. Intell. Comput., 3rd Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr. (DASC/PiCom/DataCom/CyberSciTech)*, Nov. 2017, pp. 257–262.

[44] D. Muniraj and M. Farhood, "Detection and mitigation of actuator attacks on small unmanned aircraft systems," *Control Eng. Pract.*, vol. 83, pp. 188–202, Feb. 2019.

[45] T. Sasaki, K. Sawada, S. Shin, and S. Hosokawa, "Model based fallback control for networked control system via switched Lyapunov function," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vols. E100-A, no. 10, pp. 2086–2094, Oct. 2017.

[46] J. Hoshino, H. Kojima, T. Funakoshi, R. Imai, and R. Kubo, "Secure networked motion control using tampering detection observer," in *Proc. 31st Int. Tech. Conf. Circuits/Syst., Comput. Commun. (ITC-CSCC)*, Jul. 2016, pp. 613–616.

[47] J. Hoshino, T. Funakoshi, K. Yamada, and R. Kubo, "Networked motion control with tamper detection observer and Smith predictor," in *Proc. Int. Symp. Nonlinear Theory Appl. (NOLTA)*, Dec. 2017, pp. 62–65.

[48] R. Kubo, "Detection and mitigation of false data injection attacks for secure interactive networked control systems," in *Proc. IEEE Int. Conf. Intell. Saf. Robot. (ISR)*, Aug. 2018, pp. 7–12.

[49] R. Kubo, "Effects of time delays on observer-based cyberattack detection in interactive networked control systems," in *Proc. IEEE Int. Conf. Consum. Electron.-Taiwan (ICCE-TW)*, May 2019, pp. 1–2.

[50] K. Yamada, J. Hoshino, and R. Kubo, "Detection of data tampering attacks using redundant network paths with different delays for networked control systems," *Nonlinear Theory Appl.*, vol. 10, no. 2, pp. 140–156, 2019.

[51] K. Aida, K. Yamada, R. Hotchi, and R. Kubo, "Dynamic redundant path selection for tamper-tolerant networked control," in *Proc. Int. Symp. Nonlinear Theory Appl. (NOLTA)*, Dec. 2019, pp. 581–584.

[52] K. Ohnishi, M. Shibata, and T. Murakami, "Motion control for advanced mechatronics," *IEEE/ASME Trans. Mechatronics*, vol. 1, no. 1, pp. 56–67, Mar. 1996.

[53] C. L. Lai and P. L. Hsu, "Design the remote control system with the time-delay estimator and the adaptive Smith predictor," *IEEE Trans. Ind. Informat.*, vol. 6, no. 1, pp. 73–80, Feb. 2010.

[54] O. J. M. Smith, "A controller to overcome dead time," *ISA J.*, vol. 6, no. 2, pp. 28–33, Feb. 1959.

[55] R. Imai and R. Kubo, "Experimental validation of communication disturbance observer for networked control systems with information losses," *IEICE Commun. Exp.*, vol. 5, no. 4, pp. 102–107, 2016.

[56] R. Imai and R. Kubo, "Introducing jitter buffers in networked control systems with communication disturbance observer under time-varying communication delays," in *Proc. 41st Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Nov. 2015, pp. 2956–2961.

KENTO AIDA received the B.E. degree in electronics and electrical engineering and the M.E. degree in integrated design engineering from Keio University, Japan, in 2019 and 2021, respectively.

KENTA YAMADA received the B.E. degree in electronics and electrical engineering and the M.E. degree in integrated design engineering from Keio University, Japan, in 2017 and 2019, respectively.

RYOSUKE HOTCHI received the B.E. degree in electronics and electrical engineering and the M.E. and Ph.D. degrees in integrated design engineering from Keio University, Japan, in 2016, 2018, and 2021, respectively. In 2021, he joined the Secure System Research Laboratories, NEC Corporation, Japan. His research interests include network control and queue control systems.

RYOGO KUBO (Member, IEEE) received the B.E. degree in system design engineering and the M.E. and Ph.D. degrees in integrated design engineering from Keio University, Japan, in 2005, 2007, and 2009, respectively. In 2007, he joined the NTT Access Network Service Systems Laboratories, NTT Corporation, Japan. Since 2010, he has been with Keio University, Japan, where he is currently an Associate Professor with the Department of Electronics and Electrical Engineering. From 2019 to 2020, he also held the position of a Honorary Research Fellow with the Department of Electronic and Electrical Engineering, University College London (UCL), U.K. His research interests include system control, optical communications, networking, and cyber-physical systems.

He is a Member of the Optica, the Institute of Electrical Engineers of Japan (IEEJ), the Institute of Electronics, Information and Communication Engineers (IEICE), and the Society of Instrument and Control Engineers (SICE). He received the Best Paper Award from the IEICE Communications Society, in 2011, the IEEE International Conference on Communications (ICC '12) Best Paper Award, in 2012, the Leonard G. Abraham Prize from the IEEE Communications Society, in 2013, and the 2018 IEEE International Conference on Intelligence and Safety for Robotics (ISR '18) Best Paper Award, in 2018.