Received March 18, 2022, accepted April 4, 2022, date of publication April 18, 2022, date of current version May 2, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3168128

A Generalized Hold Based Countermeasure Against Zero-Dynamics Attack With Application to DC-DC Converter

BUMSU KIM, (Graduate Student Member, IEEE),
KUNHEE RYU, (Graduate Student Member, IEEE),
AND JUHOON BACK, (Member, IEEE)
School of Robotics, Kwangwoon University, Nowon-gu, Seoul 01897, South Korea

Corresponding author: Juhoon Back (backhoon@kw.ac.kr)

This work was supported in part by the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea Government (Ministry of Trade, Industry and Energy) (20204030200010, Graduate Track for Core Technologies of Wind Power System Engineering), and in part by the Excellent researcher support project of Kwangwoon University in 2021.

ABSTRACT Zero-dynamics attack (ZDA) is a model based cyber attack. It is stealthy in the sense that the existence of attack signal cannot be determined by monitoring the system output, and it is effective to systems that have unstable zero-dynamics. Several countermeasures against ZDA have been introduced, and the one employing the generalized hold (GH) is considered in this paper. The GH is a generalized version of zero-order hold that is commonly used in the digital control systems. In this paper, the lethality of ZDA and the effectiveness of GH as a countermeasure are demonstrated on a control system that involves a DC-DC converter. Through extensive simulations and experiments, the design of the proposed scheme is presented in detail and relevant practical issues are discussed.

INDEX TERMS Cyber-physical system, generalized hold, sampled-data system, system security, zero-dynamics attack.

I. INTRODUCTION

Monitoring and controlling geographically distributed systems are essential technologies in modern engineering, and one of key ingredients that enables these is the communication network. For example, utilities companies schedule and dispatch generation through communication between suppliers and users [1], and thousands of miles of pipelines have a lot of sensors and valves that need to be monitored and controlled coordinately [2]. Obviously, it is not possible to operate these systems without communication network. Despite the tremendous benefits, the presence of network makes the systems vulnerable to cyber attacks. Well known instances of cyber attacks include Stuxnet on Iranian nuclear facilities, massive blackouts at South American power plants, and cyber attacks on the Ukrainian power grid SCADA, [3]–[6], which results in social and economic losses [3], [7], [8].

A number of cyber attacks have been reported in the literature, for example, false data injection attack [9], denial-of-service (DoS) [10], zero-dynamics attack (ZDA) [11]; see the papers and references therein for details. Among these cyber attacks, ZDA gained plenty of attention in the control system society [11]–[19] and is considered in this paper. This attack exploits the zero-dynamics of the system, which describes the internal behavior of a system, in a way that the attack signal is constructed from a dynamics that is identical to the zero-dynamics of the given system. If the system has unstable zero-dynamics, then the attack signal will drive the internal state of the system unbounded while the presence of attack signal cannot be detected by monitoring the system output. In this respect, ZDA is classified as a *stealthy* actuator attack [12], [20]. It is noted that robust versions of ZDA for linear systems [21] and nonlinear systems [22] have been proposed, which do not require complete knowledge on the system dynamics and increased the threat of ZDA significantly.

Several countermeasures against ZDA have been reported in the literature. In [23], the authors proposed a modulation

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

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

matrix based approach. This matrix can be regarded as an additional input gain that explains how the input affects the dynamics of the system, and this information is kept confidential. A time-varying modulation matrix was also introduced to increase the security. In [24], the authors presented a dual rate control scheme as a defense strategy against ZDA. It was proposed to sample the system output at a higher rate than the control signal generated. Moreover, it has been shown that this can stabilize the zero-dynamics of the closed-loop system.

A countermeasure employing the generalized hold (GH) [25] was studied in [26]. This approach is motivated by the fact that if GH is used instead of the zero-order hold (ZOH), then the zeros of the sampled-data system can be assigned at any desired locations. As a solution to the security problem, the authors proposed a design procedure to place all the zeros inside the unit circle so that the modified system does not have any unstable zero, implying that ZDA is not effective anymore. Recently, an approach using the generalized sampler (GS) [25] was presented in [27] and [28]. In this approach, the sampler that samples the output at each sampling time is replaced by GS, which can be regarded as a filter that processes more samples between the sampling time. It is known that GS can also place the zeros at any desired locations and the same idea used in the work [26] is applied to develop a countermeasure against ZDA.

Literature containing experimental results on cyber attacks can be summarized as follows. In [29] and [12], the authors reported experimental results on several cyber attacks, such as replay attack, bias injection attack, and ZDA. The target system of the cyber attacks is a quadruple tank system controlled over a network, attracting considerable amount of attention to ZDA.

The authors in [14] proposed a detection (and defense) strategy based on multirate sampling, and demonstrated the strategy on a quadrotor system. In the experiment, it is shown that the proposed strategy can detect ZDA faster than single-rate detection method. In [30], the authors dealt with the zero sum attack which is one of the stealth attacks, and reported experimental results on DC microgrid.

In this paper, we are concerned with the security of DC-DC converters controlled through a communication network and it is motivated by the fact that remote control problem on this system is an active research topic [31]–[33]. Clearly, this system is also exposed to cyber attacks and we focus on ZDA. By conducting a laboratory-scale experiment, we show that a DC-DC converter controlled over a network can be vulnerable to ZDA. In addition, we propose a GH based countermeasure for the DC-DC converter, which enhances security against ZDA.

The contributions of the paper are summarized as follows.

- It is shown that a DC-DC converter controlled over a network can have unstable zeros and is therefore vulnerable to ZDA.
- The lethality of ZDA to the converter has been verified with a laboratory-scale experimental system.

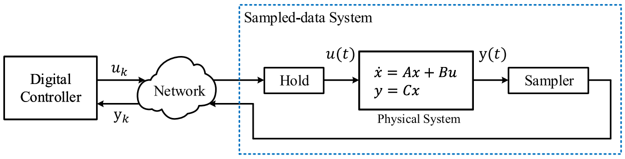


FIGURE 1. Networked control system.

- A GH is designed considering the dynamics of DC-DC converter and it is experimentally verified that the GH-based defense strategy can neutralize (or detect) ZDA on the converter.

The rest of the paper is organized as follows. Section II briefly summarizes ZDA and GH, and presents a design procedure for a particular class of GH. The DC-DC converter used in the paper is explained in Section III. Section IV describes how a ZDA can be designed and demonstrates through simulations that the attack is effective. In Section V, a countermeasure employing GH is designed for the DC-DC converter, and it is validated numerically. Section VI explains the attack and defense scenarios used in the experiments and presents the experimental results showing the effectiveness of the proposed scheme. Finally, we conclude and discuss future work in section VII.

II. PRELIMINARIES

A. ZERO-DYNAMICS ATTACK ON A NETWORKED CONTROL SYSTEM

Consider a linear system given by

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

where $x(t) \in \mathbb{R}^n$ is the state, $u(t) \in \mathbb{R}$ is the input, and $y(t) \in \mathbb{R}$ denotes the output. Suppose that the continuous-time system (1) is controlled remotely by a digital controller as shown in Fig. 1. The system and controller are connected by a communication network through which the plant output $y(t)$ and control input $u(t)$ are transmitted at each sampling time $t = kT_s$, where $T_s > 0$ is the sampling period. Based on the measurements, a control input is generated from the digital controller and transmitted to the system. In what follows, u_k and y_k stand for $u(kT_s)$ and $y(kT_s)$, respectively. The input is applied to the continuous-time system by using the hold device that converts the discrete-time control input into a continuous-time control input, i.e., $u(t) := u_k$ for $kT_s \le t < (k+1)T_s$. In this case, the sampled-data system of (1) becomes

$$\begin{aligned} x_{k+1} &= A_{\mathsf{d}}x_k + B_{\mathsf{d}}u_k \\ y_k &= C_{\mathsf{d}}x_k \end{aligned} \tag{2}$$

where $x_k = x(kT_s)$, $A_{\mathsf{d}} = e^{AT_s}$, $B_{\mathsf{d}} = \int_0^{T_s} e^{A(T_s-\tau)}Bd\tau$, and $C_{\mathsf{d}} = C$.

The security problem under consideration is closely related to the internal dynamics of a system and this dynamics can be clearly identified once the system is rewritten in the

Byrnes-Isidori normal form [34]. Precisely, there exists a coordinate transform

$$\begin{bmatrix} \eta_k \\ \xi_k \end{bmatrix} = Tx_k \tag{3}$$

which transforms the system (2) into the normal form given by

$$\begin{aligned} \begin{bmatrix} \eta_{k+1} \\ \xi_{k+1} \end{bmatrix} &= \begin{bmatrix} S_\mathrm{d} & P_\mathrm{d}\bar{C}_\mathrm{d} \\ \bar{B}_\mathrm{d}\psi_\mathrm{d}^\top & \bar{A}_\mathrm{d} + \bar{B}_\mathrm{d}\phi_\mathrm{d}^\top \end{bmatrix} \begin{bmatrix} \eta_k \\ \xi_k \end{bmatrix} + \begin{bmatrix} 0_{n-\rho} \\ \bar{B}_\mathrm{d} g_\mathrm{d} \end{bmatrix} u_k \\ &=: \tilde{A}_\mathrm{d} \begin{bmatrix} \eta_k \\ \xi_k \end{bmatrix} + \tilde{B}_\mathrm{d} u_k \\ y_k &= \begin{bmatrix} 0_{n-\rho}^\top & \bar{C}_\mathrm{d} \end{bmatrix} \begin{bmatrix} \eta_k \\ \xi_k \end{bmatrix} \end{aligned} \tag{4}$$

where ρ is the relative degree of the system, $\eta_k \in \mathbb{R}^{n-\rho}$ and $\xi_k \in \mathbb{R}^{\rho}$ are vectors corresponding to the internal and external state of the system, respectively, and $0_{n-\rho} \in \mathbb{R}^{n-\rho}$ denotes the zero vector. In addition,

$$\bar{A}_\mathrm{d} = \begin{bmatrix} 0_{\rho-1} & I_{\rho-1} \\ 0 & 0_{\rho-1}^\top \end{bmatrix}, \bar{B}_\mathrm{d} = \begin{bmatrix} 0_{\rho-1} \\ 1 \end{bmatrix}, \bar{C}_\mathrm{d} = \begin{bmatrix} 1 & 0_{\rho-1}^\top \end{bmatrix},$$

and P_d, S_d, ψ_d, ϕ_d, and g_d are the parameters that are uniquely determined by A_d, B_d, C_d, and ρ.

Let us explain the internal dynamics in more detail. Noting that the output y_k depends only on the state ξ_k, we can construct an input u_k that results in a nontrivial behavior of η_k while y_k is identically zero. In fact, when $\xi_0 = 0$, the input $u_k = \frac{1}{g_\mathrm{d}}(-\psi_\mathrm{d}^\top \eta_k - \phi_\mathrm{d}^\top \xi_k)$ yields $\xi_{k+1} = \bar{A}_\mathrm{d}\xi_k$ and $\eta_{k+1} = S_\mathrm{d}\eta_k$, meaning that the input completely decouples the dynamics of ξ_k and η_k and the behavior of η_k cannot be observed from system output. The internal dynamics $\eta_{k+1} = S_\mathrm{d}\eta_k$ is called the zero-dynamics of the system since the eigenvalues of S_d correspond to the zeros of the transfer function of (2) [34].

Suppose that A_d is Schur stable and let η_0 and ξ_0 be the initial condition of the system. Then, from the fact that $\tilde{A}_\mathrm{d}$ is also Schur stable, it follows that, under zero input ($u_k = 0$) there exist $\kappa > 0$ and $|\lambda| < 1$ such that

$$\left\| \begin{bmatrix} \eta_k \\ \xi_k \end{bmatrix} \right\| \leq \kappa\lambda^k \left\| \begin{bmatrix} \eta_0 \\ \xi_0 \end{bmatrix} \right\|,$$

and this property will be used shortly when we discuss the effect of ZDA.

ZDA targets the networked control systems, exploiting vulnerability that arises from the presence of the network. Now, suppose that a malicious attacker can inject an attack signal into the input channel. Then, the system (1) under ZDA is given by

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B(u(t) + a(t)) \\ y(t) &= Cx(t) \end{aligned} \tag{5}$$

where $a(t) \in \mathbb{R}$ is the attack signal. Similar to (2), the sampled-data system of (5) becomes

$$\begin{aligned} x_{k+1} &= A_\mathrm{d}x_k + B_\mathrm{d}(u_k + a_k) \\ y_k &= C_\mathrm{d}x_k. \end{aligned} \tag{6}$$

Assuming that the attacker has acquired the system parameters S_d, g_d, and ψ_d, the ZDA is constructed as

$$\zeta_{k+1} = S_\mathrm{d}\zeta_k, \quad a_k = -\frac{1}{g_\mathrm{d}}\psi_\mathrm{d}^\top \zeta_k, \tag{7}$$

where $\zeta_k \in \mathbb{R}^{n-\rho}$ is the state of the attack generator. Then, in the coordinates (η_k, ξ_k) defined in (3), we have

$$\begin{aligned} \eta_{k+1} &= S_\mathrm{d}\eta_k + P_\mathrm{d}\bar{C}_\mathrm{d}\xi_k \\ \xi_{k+1} &= (\bar{A}_\mathrm{d} + \bar{B}_\mathrm{d}\phi_\mathrm{d}^\top)\xi_k + \bar{B}_\mathrm{d}\psi_\mathrm{d}^\top(\eta_k - \zeta_k) + \bar{B}_\mathrm{d}g_\mathrm{d}u_k \\ y_k &= \bar{C}_\mathrm{d}\xi_k. \end{aligned}$$

From the fact that the system matrix of η_k-dynamics is identical to that of ζ_k-dynamics, we have

$$\begin{aligned} \begin{bmatrix} \eta_{k+1} - \zeta_{k+1} \\ \xi_{k+1} \end{bmatrix} &= \tilde{A}_\mathrm{d} \begin{bmatrix} \eta_k - \zeta_k \\ \xi_k \end{bmatrix} + \tilde{B}_\mathrm{d}u_k \\ y_k &= \begin{bmatrix} 0_{n-\rho}^\top & \bar{C}_\mathrm{d} \end{bmatrix} \begin{bmatrix} \eta_k - \zeta_k \\ \xi_k \end{bmatrix}. \end{aligned} \tag{8}$$

Since $\tilde{A}_\mathrm{d}$ is Schur stable by assumption, we have, under $u_k = 0$ for all $k \geq 0$, that

$$\left\| \begin{bmatrix} \eta_k - \zeta_k \\ \xi_k \end{bmatrix} \right\| \leq \kappa\lambda^k \left\| \begin{bmatrix} \eta_0 - \zeta_0 \\ \xi_0 \end{bmatrix} \right\|.$$

Above inequality implies that ξ_k and $\eta_k - \zeta_k$ converge to zero as k increases, which explains the danger of ZDA. In fact, if S_d has at least one unstable mode (S_d may be unstable even if A_d is stable), ζ_k can be unbounded by (7), which results in that η_k is also unbounded. Meanwhile, since y_k depends only on ξ_k, the divergence of the internal state cannot be observed from y_k.

It is emphasized that the stability of the zero-dynamics of the continuous-time system does not guarantee that the system is safe from ZDA. This is because of the fact that if a continuous-time system has a relative degree greater than 2 then the corresponding sampled-date system has at least one unstable zero for sufficiently small sampling period, and this zero is called the sampling zero [25].

B. GENERALIZED HOLD: A COUNTERMEASURE AGAINST ZERO-DYNAMICS ATTACK

In this subsection, we introduce GH as a countermeasure against ZDA. It is motivated by the fact that if a properly designed GH is used instead of ZOH, then the zeros of the new sampled-data system can be placed at any given desired locations.

Consider again the networked control system shown in Fig. 1. Since the controller (discrete-time system) and the system (continuous-time system) have different time domains, hold and sample devices are required, which operate as an analog-to-digital and a digital-to-analog converter, respectively.

In [25] and [35], the authors have introduced more general concept of a hold device known as GH. GH is a linear hold device with an impulse response $h(t)$, and a sampled-data system with GH is given by

$$\begin{aligned} x_{k+1} &= A_{\mathsf{d}} x_k + B_g u_k \\ y_k &= C_{\mathsf{d}} x_k \end{aligned} \tag{9}$$

where $A_{\mathsf{d}} = e^{AT_s}$, $B_g = \int_0^{T_s} e^{A(T_s-\tau)} Bh(\tau) d\tau$, and $C_{\mathsf{d}} = C$. Note that ZOH is a special case of GH in which impulse response is given by $h_g(t) = 1, t \in [0, T_s)$ and $h_g(t) = 0$ otherwise. It is known that the zeros of (9) can be located arbitrarily by properly designing $h_g(t)$, and one can neutralize the ZDA by selecting the desired zeros inside the unit circle [26], [36].

We consider the piecewise constant GH [36] which can be implemented easily compared to general continuous ones. Suppose that the pair $(A_{\mathsf{d}}, C_{\mathsf{d}})$ is observable, and let $h_g(t)$ be given by

$$h_g(t) = \begin{cases} h_i, & t \in \left[\frac{(i-1)T_s}{N}, \frac{iT_s}{N}\right), \ 1 \le i \le N, \\ 0, & \text{otherwise}, \end{cases}$$

where N is the number of subintervals. During each subinterval, GH generates a continuous-time signal $u(t) = h_i u_k$ as depicted in Fig. 2b.

The design of $h_g(t)$ is done by choosing the gains h_i and this can be done as follows.

Design procedure

1. Choose $N \ge n$ and the desired zeros $z_{d,1}, \ldots, z_{d,n-1}$ such that $|z_{d,i}| < 1, i = 1, \ldots, n-1$. Construct

$$G^*_{\mathsf{d}}(z) = k_{\mathsf{d}} \frac{(z - z_{d,1}) \cdots (z - z_{d,n-1})}{\det(zI_n - A_{\mathsf{d}})} := k_{\mathsf{d}} \tilde{G}^*_{\mathsf{d}}(z)$$

where $k_{\mathsf{d}} \in \mathbb{R}$ is a gain.

2. Realize $\tilde{G}^*_{\mathsf{d}}(z)$ in controllable canonical form

$$\begin{aligned} x_{k+1} &= A_{\mathsf{ctr}} x_k + B_{\mathsf{ctr}} u_k \\ y_k &= C_{\mathsf{ctr}} x_k, \end{aligned} \tag{10}$$

and obtain A_{ctr}, B_{ctr}, and C_{ctr}.

3. Calculate the observability matrices $\mathcal{O}_{\mathsf{d}}$ of $(A_{\mathsf{d}}, C_{\mathsf{d}})$ and $\mathcal{O}_{\mathsf{ctr}}$ of $(A_{\mathsf{ctr}}, C_{\mathsf{ctr}})$ as

$$O_{\mathsf{d}} = \begin{bmatrix} C_{\mathsf{d}} \\ C_{\mathsf{d}} A_{\mathsf{d}} \\ \vdots \\ C_{\mathsf{d}} A_{\mathsf{d}}^{n-1} \end{bmatrix}, \ O_{\mathsf{ctr}} = \begin{bmatrix} C_{\mathsf{ctr}} \\ C_{\mathsf{ctr}} A_{\mathsf{ctr}} \\ \vdots \\ C_{\mathsf{ctr}} A_{\mathsf{ctr}}^{n-1} \end{bmatrix}.$$

Compute

$$B_g = \mathcal{O}_{\mathsf{d}}^{-1} \mathcal{O}_{\mathsf{ctr}} B_{\mathsf{ctr}}.$$

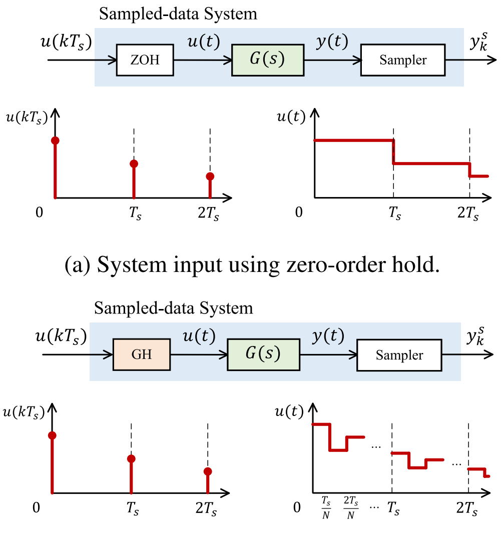
4. Find $\bar{h}$ using $\bar{h} = C^{\dagger}_{\mathsf{d},N} B_g$ where

$$\begin{aligned} A_{\mathsf{d},N} &= e^{A\frac{T_s}{N}}, \ B_{\mathsf{d},N} = \int_0^{\frac{T_s}{N}} e^{A(\frac{T_s}{N}-\tau)} B d\tau \\ C_{\mathsf{d},N} &= \left[A^{N-1}_{\mathsf{d},N} B_{\mathsf{d},N} \cdots B_{\mathsf{d},N} \right], \end{aligned}$$

and $C^{\dagger}_{\mathsf{d},N}$ denotes Moore-Penrose pseudo inverse of $C_{\mathsf{d},N} \in \mathbb{R}^{n \times N}$.

5. Find $h := [h_1 \ \cdots \ h_N]^{\top}$ such that $h_i = k_d \bar{h}_i$ where $k_d = N / \sum_{i=1}^{N} \bar{h}_i$ and $\bar{h}_i$ is the i-th element of $\bar{h}$.

The above design procedure constructively determines the gains for GH so that the transfer function of (9) becomes identical to $G^*_{\mathsf{d}}(z)$. See [26], [36] for more details.



(a) System input using zero-order hold.

(b) System input using generalized hold.

FIGURE 2. Input signals generated by zero-order hold and generalized hold.

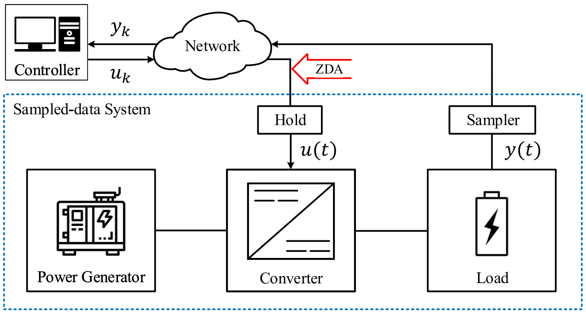


FIGURE 3. Control system under zero-dynamics attack.

III. DC-DC CONVERTER CONTROL SYSTEM: EXPERIMENTAL PLATFORM

The main objective of this paper is to demonstrate that systems that are controlled over a network are vulnerable to ZDA and a GH based countermeasure can protect the systems from ZDA. A DC-DC converter control system is chosen to validate the idea since it is widely used in various engineering systems and it is common to control this system using a digital controller which generates a control input and send it to the actuator through a network.

Consider a power generation system shown in Fig. 3 in which a DC-DC converter controls the power flow between a generator and load, and the DC-DC converter is controlled by a digital controller. The controller produces a control input

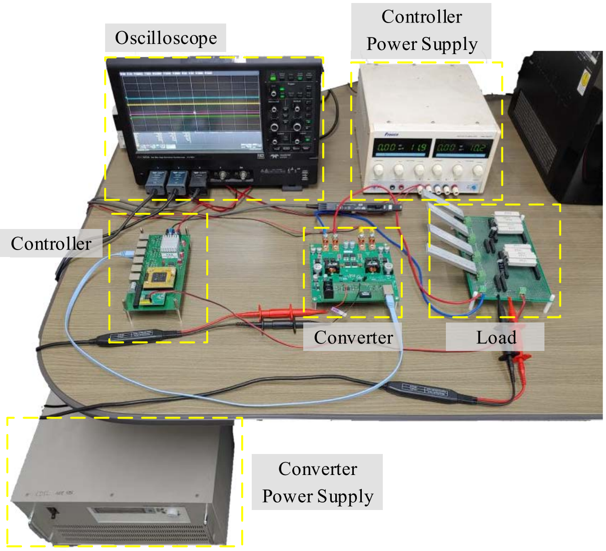
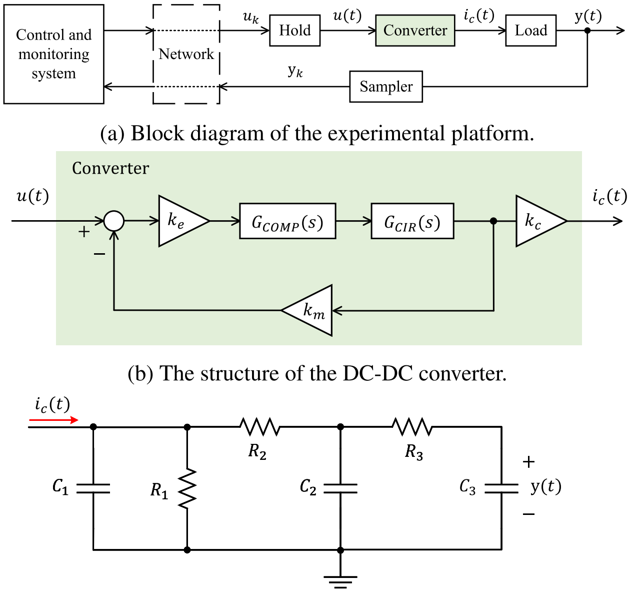


FIGURE 4. Experimental platform.



(a) Block diagram of the experimental platform.

(b) The structure of the DC-DC converter.

(c) Load circuit.

FIGURE 5. Experimental platform configuration.

u_k and sends it to the converter through a communication network, and a hold device generates a continuous-time input signal $u(t)$. The continuous-time output of the system $y(t)$ is sampled by a sampler, and it is transmitted to the controller for feedback. We suppose that an attacker with a malicious purpose can inject an attack signal a_k so that the actual input signal transmitted to the hold device is $u_k + a_k$ rather than u_k, i.e., the actual input $u(t)$ applied to the system will be generated from $u_k + a_k$.

In this paper, the cyber attack scenario described above is studied using a lab-scale control system. In what follows, we describe the components and explain mathematical models that are used to construct a ZDA and its countermeasure.

A. SYSTEM CONFIGURATION

The system shown in Fig. 4 is the experimental platform with which our theory is demonstrated. It consists of a power supply, converter, load, and a digital controller. The signal flow between components is described in Fig. 5a. The power supply (TPE-25010S, Toyotech Co., Ltd.) keeps the input voltage applied to the converter at 48 V. The converter (LM5170-Q1, Texas Instruments) outputs the current $i_c(t)$, which is generated by adding the currents from two channels ($k_c = 2$ explains this). The maximum output current is 30 A when the control input is 0.75 V.

Fig. 5b shows the structure of the converter. The converter consists of a compensator and a switching circuit, whose transfer functions are denoted by $G_{COMP}(s)$ and $G_{CIR}(s)$, respectively. It also has an error amplifier whose transconductance is denoted by k_e (represented as a gain in the block diagram), and a current sense amplifier whose gain is k_m.

The converter has a load that is represented by a resistor-capacitor circuit; see Fig. 5c. The input of the load is the output current of the converter, and the output of the load is the voltage across the capacitor C_3, denoted by $y(t)$. The load circuit can be interpreted as a case in which a capacitor C_1, a resistor R_1, and a battery [37] are connected in parallel.

A proportional-integral (PI) type controller is implemented in the micro-controller (TMS320F28335, Texas Instruments) and it regulates the error between the reference $v_{ref}(t)$ and the system output y_k. The gains are given by $k_p = 3$ and $k_i = 1$. The controller sends the generated control input to the converter, and it receives the sampled output voltage y_k through the network.

B. SYSTEM MODELING

Since the controller is a discrete-time system, hold and sample devices are required to interface the controller and plant. The input of the converter $u(t)$ is generated by the hold device in the micro-controller. The sample device, which converts $y(t)$ to y_k, used in our experiments is a voltage sensor (AD7607, Analog Devices, ±10 V of measurement range). At each sampling time, the controller receives the measurement y_k from this device.

In this subsection, we derive a mathematical model of the experimental platform shown in Fig. 4. We find transfer functions of the DC-DC converter and the load, and compare the step responses of the model and experimental system.

According to the manufacturer's document (LM5170-Q1 datasheet), the transfer functions of the compensator and the switching circuit of the converter (see Fig. 5b) are given by

$$\begin{aligned} G_{COMP}(s) &= \frac{9.51 \times 10^{-6}s + 1}{9.51 \times 10^{-15}s^2 + 1.5 \times 10^{-8}s} \\ G_{CIR}(s) &= \frac{0.104}{4.7 \times 10^{-6}s + 0.1}. \end{aligned} \tag{11}$$

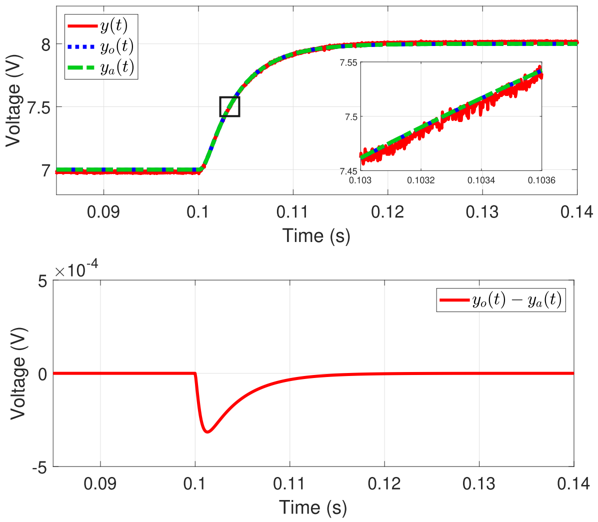


FIGURE 6. **Model validation using experimental data. Step responses of experimental system, converter model $\bar{G}(s)$, a simplified model $G(s)$ of $\bar{G}(s)$ (top). Output error between $\bar{G}(s)$ and $G(s)$ (bottom).**

It can be seen that the converter is a negative feedback system consisting of $k_e G_{COMP}(s) G_{CIR}(s)$ in the forward loop and k_m in the feedback loop. Let $I_c(s)$ and $U(s)$ be the Laplace transforms of $i_c(t)$ and $u(t)$, respectively. Then, the transfer function of the converter $G_{CONV}(s) := \frac{I_c(s)}{U(s)}$ becomes

$$G_{CONV}(s) = \frac{k_c k_e G_{COMP}(s) G_{CIR}(s)}{1 + k_e k_m G_{COMP}(s) G_{CIR}(s)} \tag{12}$$

where $k_c = 2$, $k_e = 0.001$, and $k_m = 0.05$. The numerical values are taken from manufacturer's document (LM5170-Q1 datasheet).

Fig. 5c shows the load circuit in the system. Let $Y(s)$ be the Laplace transform of $y(t)$. A simple analysis of the circuit gives

$$\frac{Y(s)}{I_c(s)} := G_{LOAD}(s) = \frac{b_{L,0}}{a_{L,3}s^3 + a_{L,2}s^2 + a_{L,1}s + a_{L,0}} \tag{13}$$

where $a_{L,3} = R_1R_2R_3C_1C_2C_3$, $a_{L,2} = R_1R_2C_1C_2 + R_1R_3C_1C_3 + R_1R_2C_1C_3 + R_1R_3C_2C_3 + R_2R_3C_2C_3$, $a_{L,1} = R_1C_1 + R_1C_2 + R_1C_3 + R_2C_2 + R_2C_3 + R_3C_3$, $a_{L,0} = 1$, $b_{L,0} = R_1$. The parameters are given by $R_1 = 0.5$ Ω, $R_2 = 1$ Ω, $R_3 = 1$ Ω, $C_1 = 739$ μF, $C_2 = 1$ mF, $C_3 = 1$ mF.

From (12) and (13), we have

$$\begin{aligned} \frac{Y(s)}{U(s)} &=: \bar{G}(s) = G_{CONV}(s) G_{LOAD}(s) \\ &= \frac{\bar{b}_1 s + \bar{b}_0}{\bar{a}_6 s^6 + \cdots + \bar{a}_1 s + \bar{a}_0} \end{aligned} \tag{14}$$

where $\bar{a}_6 = 3.44 \times 10^{-30}$, $\bar{a}_5 = 5.44 \times 10^{-24}$, $\bar{a}_4 = 4.49 \times 10^{-19}$, $\bar{a}_3 = 3.99 \times 10^{-14}$, $\bar{a}_2 = 2.66 \times 10^{-10}$, $\bar{a}_1 = 4.38 \times 10^{-7}$, $\bar{a}_0 = 1.0 \times 10^{-4}$, $\bar{b}_1 = 1.90 \times 10^{-8}$, $\bar{b}_0 = 2.0 \times 10^{-3}$.

From the numerical values of the system, it is seen that the converter part is much faster than the load part. In fact, the poles of $G_{CONV}(s)$ are given by -1.56×10^6 and $-3.73 \times 10^4 \pm j7.59 \times 10^4$, while $G_{LOAD}(s)$ has poles at -4.63×10^3, -2.16×10^3, and -2.71×10^2. Based on this observation, we approximate $G_{CONV}(s)$ as a constant $g_{conv} = G_{CONV}(0) = 40$, and obtain a simplified model $G(s)$ of $\bar{G}(s)$ as

$$G(s) = g_{conv} G_{LOAD}(s).$$

The numerical models $G(s)$ and $\bar{G}(s)$ are quite accurate in the sense that the step responses have little difference compared with that of experimental system. The step responses are shown in Fig. 6 and it is observed that the difference between the step responses of $\bar{G}(s)$ and $G(s)$ is less than -5×10^{-4}.

To proceed, we obtain a sampled-data model of $G(s)$. Suppose that ZOH is used as a hold device and $T_s = 0.8$ ms. Then, we have

$$G_{\mathsf{d}}(z) = \frac{b_{\mathsf{d},2}z^2 + b_{\mathsf{d},1}z + b_{\mathsf{d},0}}{z^3 + a_{\mathsf{d},2}z^2 + a_{\mathsf{d},1}z + a_{\mathsf{d},0}} \tag{15}$$

where $a_{\mathsf{d},2} = -1.01$, $a_{\mathsf{d},1} = 1.68 \times 10^{-1}$, $a_{\mathsf{d},0} = -3.53 \times 10^{-3}$, $b_{\mathsf{d},2} = 1.37$, $b_{\mathsf{d},1} = 1.67$, $b_{\mathsf{d},0} = 8.47 \times 10^{-2}$.

In this paper, we assume that the system is operating at $u_{\text{op}} = 0.375$ V and $y_{\text{op}} = 7.5$ V. Thus, the linear models $G(s)$ and $\bar{G}(s)$ are obtained around this operating condition and the actual control input applied to the DC-DC converter is expressed as

$$u(t) := u_c(t) + u_{\text{offset}}$$

where $u_{\text{offset}} = 0.375$ V corresponds to the input at the operating point and $u_c(t)$ is the control input generated by the hold device.

IV. ZERO-DYNAMICS ATTACK ON DC-DC CONVERTER

In this section, we consider a situation that an attacker injects ZDA to the control system shown in Fig. 4. The construction of attack signal is explained in detail and the effect of the attack is demonstrated by numerical simulations.

Suppose that $G_{\mathsf{d}}(z)$ given in (15) is exposed to the attacker. Let $D_{\mathsf{d}}(z)$ (assumed to be monic) and $N_{\mathsf{d}}(z)$ be the denominator and numerator of $G_{\mathsf{d}}(z)$, respectively, namely

$$G_{\mathsf{d}}(z) = \frac{N_{\mathsf{d}}(z)}{D_{\mathsf{d}}(z)}.$$

Dividing $D_{\mathsf{d}}(z)$ by $N_{\mathsf{d}}(z)$ results in that

$$D_{\mathsf{d}}(z) = Q_{\mathsf{d}}(z) N_{\mathsf{d}}(z) + R_{\mathsf{d}}(z) \tag{16}$$

where $Q_{\mathsf{d}}(z) = 0.73z - 1.62$ and $R_{\mathsf{d}}(z) = 2.82z + 0.13$. We then rewrite $G_{\mathsf{d}}(z)$ as

$$G_{\mathsf{d}}(z) = \frac{N_{\mathsf{d}}(z)}{Q_{\mathsf{d}}(z) N_{\mathsf{d}}(z) + R_{\mathsf{d}}(z)} = \frac{\frac{1}{Q_{\mathsf{d}}(z)}}{1 + \frac{1}{Q_{\mathsf{d}}(z)} \frac{R_{\mathsf{d}}(z)}{N_{\mathsf{d}}(z)}},$$

which can be regarded as the transfer function of a closed-loop system that is composed of two systems with transfer functions $\frac{1}{Q_{\mathsf{d}}(z)}$ and $\frac{R_{\mathsf{d}}(z)}{N_{\mathsf{d}}(z)}$, as shown in Fig. 7.

We now realize the transfer functions $\frac{R_\mathsf{d}(z)}{N_\mathsf{d}(z)}$ and $\frac{1}{Q_\mathsf{d}(z)}$ in the state space as follows. First, the transfer function $\frac{R_\mathsf{d}(z)}{N_\mathsf{d}(z)}$ is realized in the controllable canonical form, i.e.,

$$\begin{aligned}\eta_{k+1} &= \begin{bmatrix} 0 & 1 \\ -0.06 & -1.22 \end{bmatrix} \eta_k + \begin{bmatrix} 0 \\ 1 \end{bmatrix} y_k \\ &=: S_\mathsf{d}\eta_k + P_\mathsf{d} y_k \\ \omega_k &= \begin{bmatrix} -0.13 & -2.82 \end{bmatrix} \eta_k \\ &=: \psi_\mathsf{d}^\top \eta_k \end{aligned} \tag{17}$$

where $\eta_k \in \mathbb{R}^2$ is the state and $\omega_k \in \mathbb{R}$ is the output of the subsystem. It is noted that the eigenvalues of S_d correspond to the zeros of $N_\mathsf{d}(z)$ (equivalently $G_\mathsf{d}(z)$) and hence the dynamics of η with $y_k \equiv 0$ is the zero-dynamics of $G_\mathsf{d}(z)$.

Meanwhile, one can realize $\frac{1}{Q_\mathsf{d}(z)}$ as

$$\begin{aligned}\xi_{k+1} &= 2.23\xi_k + 1.37\, e_k \\ &=: \phi_\mathsf{d}^\top \xi_k + g_\mathsf{d} e_k \\ y_k &= \xi_k \end{aligned} \tag{18}$$

where $\xi_k \in \mathbb{R}$ is the state and $e_k := u_k - \omega_k$. Then, from (17) and (18), the transfer function $G_\mathsf{d}(z)$ is realized in normal form given by

$$\begin{aligned}\begin{bmatrix} \eta_{k+1} \\ \xi_{k+1} \end{bmatrix} &= \begin{bmatrix} S_\mathsf{d} & P_\mathsf{d} \\ -g_\mathsf{d}\psi_\mathsf{d}^\top & \phi_\mathsf{d}^\top \end{bmatrix} \begin{bmatrix} \eta_k \\ \xi_k \end{bmatrix} + \begin{bmatrix} 0_2 \\ g_\mathsf{d} \end{bmatrix} u_k \\ y_k &= \begin{bmatrix} 0_2^\top & 1 \end{bmatrix} \begin{bmatrix} \eta_k \\ \xi_k \end{bmatrix}. \end{aligned} \tag{19}$$

Since S_d has an unstable eigenvalue at -1.17, the system under consideration is vulnerable to ZDA in the sense that an attack generated by the dynamics (7) with any ζ_0 belonging to the eigenspace corresponding to an unstable eigenvalue of S_d will drive η_k unbounded while y_k converges to zero due to stability of the system.

The effect of ZDA is demonstrated by numerical simulations. In the simulation, we assume that the system has transfer function $\bar{G}(s)$ and a ZDA is constructed using $G(s)$. The DC-DC converter used in the experiment has an input limit (0 A to 0.75 A) and this is also considered in the simulation. In addition, a threshold of 0.1 V is set so that if the voltage deviation of the output voltage from its normal value (7.5 V) is greater than this threshold, then it is determined that an attack is present.

The attack that has been constructed from the approximate system model $G(s)$ has two state variables and is applied to the system at $T_a = 0.04$. The initial condition of ZDA is chosen as $\zeta_0 = \begin{bmatrix} -0.651 & 0.759 \end{bmatrix} \times 10^{-8}$.

Fig. 8 shows the output behavior of the system under ZDA. Since S_d has an unstable eigenvalue, the attack signal a_k diverges as k increases, and the effect of the attack appears on the continuous-time output $y(t)$. On the other hand, the sampled output y_k resides within the normal region, which implies that the monitoring system cannot recognize that the system is under attack.

It is noted that the state of zero-dynamics does not diverge but oscillates and this is due to physical limitation on the input signal. If there is no limit on the input, then the state of the zero-dynamics will diverge as is expected by the theory. Although bounded, the large oscillation in the state makes the output signal $y(t)$ exceed the threshold and this undesirable oscillation may shorten the lifetime of the circuit or cause damage and thus can be a target of malicious attack.

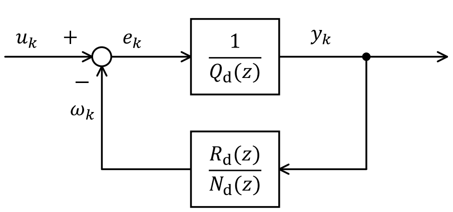

u_k
+
e_k
$\frac{1}{Q_\mathsf{d}(z)}$
y_k
−
ω_k
$\frac{R_\mathsf{d}(z)}{N_\mathsf{d}(z)}$

FIGURE 7. Feedback representation of $G_\mathsf{d}(z)$.

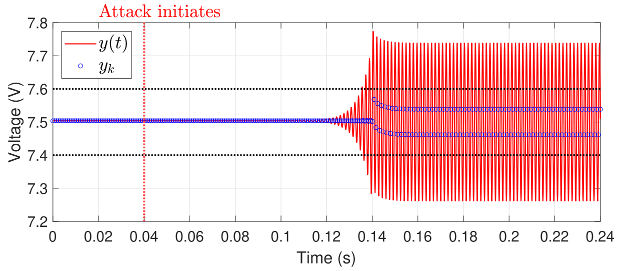


FIGURE 8. Continuous and discrete-time output of a system using zero-order hold under zero-dynamics attack based on the zero-dynamics of a system $G(s)$ using zero-order hold.

V. GENERALIZED HOLD FOR DC-DC CONVERTER

In this section, we design a GH for a DC-DC converter system and demonstrate that GH can improve security against ZDA. As explained in Section II-B, the main idea is to relocate all the zeros inside the unit circle so that the attack signal based on the new zero-dynamics converges to zero posing little threat to the system.

We follow the design procedure described in Section II-B to design a GH. In step 1, we choose $N = 4$, $z_{d,1} = -0.6$, and $z_{d,2} = 0$. Then, $\tilde{G}_\mathsf{d}^*$ becomes

$$\tilde{G}_\mathsf{d}^* = \frac{z^2 + \tilde{b}_{\mathsf{d},1} z}{z^3 + a_{\mathsf{d},2} z^2 + a_{\mathsf{d},1} z + a_{\mathsf{d},0}} \tag{20}$$

where $\tilde{b}_{\mathsf{d},1} = -z_{d,1}$. In step 2, we realize $\tilde{G}_\mathsf{d}^*$ in controllable canonical form as

$$\begin{aligned} x_{k+1} &= \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 3.5 \times 10^{-3} & -0.17 & 1.01 \end{bmatrix} x_k + \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u_k \\ &=: A_{\mathsf{ctr}} x_k + B_{\mathsf{ctr}} u_k \\ y_k &= \begin{bmatrix} 0 & 0.6 & 1 \end{bmatrix} x_k \\ &=: C_{\mathsf{ctr}} x_k. \end{aligned} \tag{21}$$

In step 3, we compute $B_g = \mathcal{O}_\mathsf{d}^{-1} \mathcal{O}_{\mathsf{ctr}} B_{\mathsf{ctr}}$ to have $B_g = \begin{bmatrix} 1 & 1.89 \times 10^3 & -3.78 \times 10^6 \end{bmatrix}^\top$. In step 4, we compute the

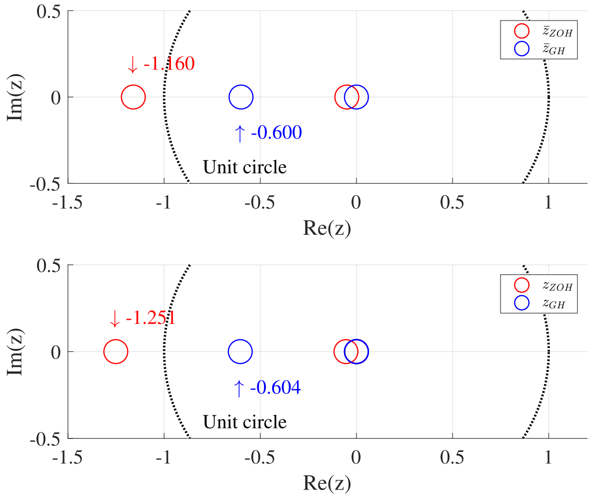


FIGURE 9. Shift of discrete-time zeros: approximated system $G(s)$ (top) and original system $\bar{G}(s)$ (bottom).

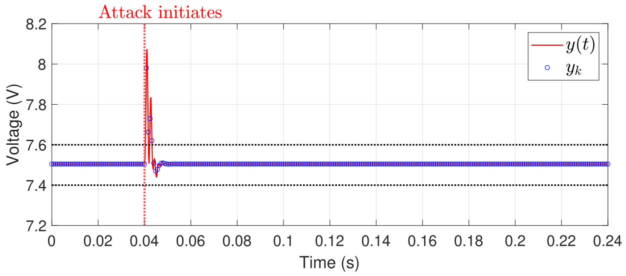


FIGURE 10. Response of the system under zero-dynamics attack. Generalized hold is used as a hold device and zero-dynamics attack is based on the new zero-dynamics.

matrix $C_{\mathsf{d},N}$ and obtain

$$\bar{h} = [9.61 \times 10^8 \;\; 1.16 \times 10^9 \;\; 1.01 \times 10^9 \;\; -3.78 \times 10^8]. \tag{22}$$

Finally, in step 5, by computing $k_d = N/\sum_{i=1}^{N} \bar{h}_i$ and using $h_i = k_d \bar{h}_i$, we have

$$h = \begin{bmatrix} 1.39 & 1.69 & 1.47 & -0.55 \end{bmatrix}. \tag{23}$$

Fig. 9 represents the zeros of the sampled-data system with ZOH and GH, respectively. The circles denote the zeros of the systems. As can be seen in the figure, one of the zeros of $G(s)$ with ZOH is located outside of the unit circle. Whereas all the zeros of $G(s)$ with GH are inside the unit circle, which implies that ZDA has little or no influence. We note that the proposed GH has robustness against plant uncertainty in the sense that although it is designed for the approximated model $G(s)$, it also places all the zeros of $\bar{G}(s)$ inside the unit circle as shown in Fig. 9.

Fig. 10 shows the response of the system $\bar{G}(s)$ under ZDA when the proposed GH is used instead of ZOH. The attack is constructed based on the zero-dynamics of $G_{\mathsf{d}}^{*}(z)$. As can be seen from the response, the ZDA has little effect on the system and this is because the attack is based on a stable zero-dynamics and thus converges to zero asymptotically.

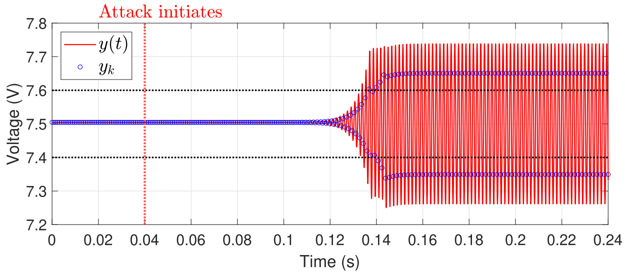


FIGURE 11. Output of a system using generalized hold under zero-dynamics attack based on the zero-dynamics of a system $G(s)$ using zero-order hold.

If the attacker insists on injecting ZDA using the unstable zero-dynamics (that of the case using ZOH), this can be recognized by the monitoring system. Fig. 11 illustrates this situation. Since the dynamics of the attack signal is no longer the same as that of the target, the effect of ZDA appears on the output so that the monitoring system can take appropriate action to protect the system.

VI. EXPERIMENTAL RESULT

This section presents the experimental results for the control system shown in Fig. 4. We consider the situation in which the system is stabilized by a PI controller that is implemented in a micro-controller. The proportional and integral gains of the controller are chosen as $k_p = 3$ and $k_i = 1$, respectively. In addition, as described in Section III-B, the values corresponding to the operating condition are given by $u_{\text{offset}} = 0.375$ V and $y_{\text{op}} = 7.5$ V. The sampling time is given by $T_s = 0.8$ ms. The output measured by an oscilloscope is denoted by $y(t)$ and the attack is initiated at $T_a = 0.04$ s.

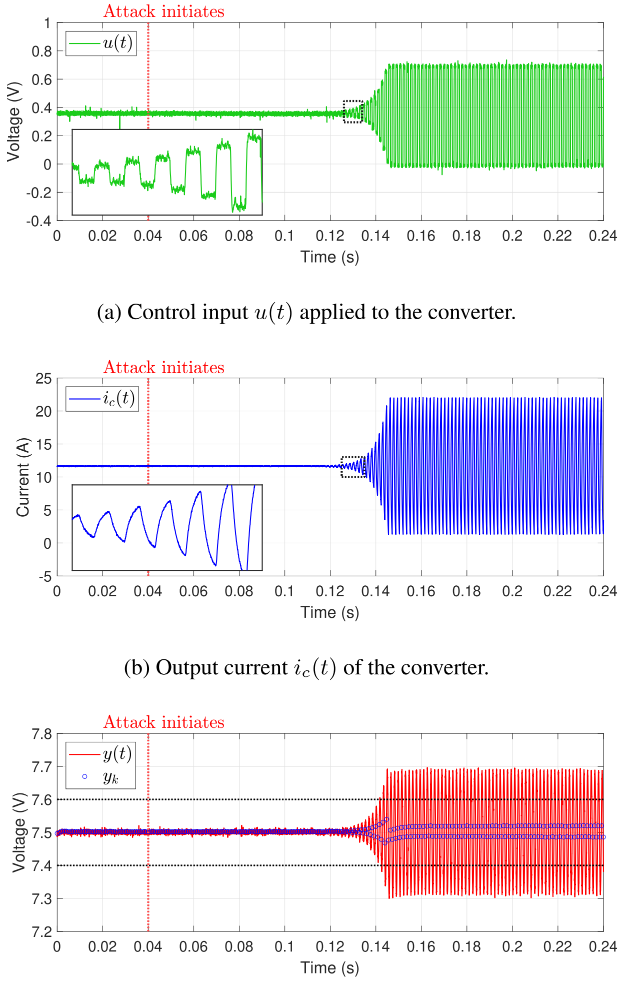
Under this configuration, we consider the following scenarios for experiment.

- Scenario 1: injecting ZOH based ZDA into the system with ZOH.
- Scenario 2: injecting GH based ZDA into the system with GH.
- Scenario 3: injecting ZOH based ZDA into the system with GH.

A. SCENARIO 1

In the first scenario, we consider a situation that an attacker injects ZDA to the system that has ZOH as the hold device. The system is vulnerable to ZDA because zero-dynamics of the system is unstable. The parameters and initial value ζ_0 of ZDA are chosen as the same values given in Section IV.

Fig. 12a shows the input signal $(u_c(t)+u_{\text{offset}}+a(t))$ applied to the converter. Before the attack is injected, a constant voltage (u_{offset}, operating condition) and control input $u_c(t)$ are applied to the converter. After $t = T_a$, it can be seen that the input voltage is affected as the attack increases. Due to the input constraints, the actual input applied to the converter $u(t)$

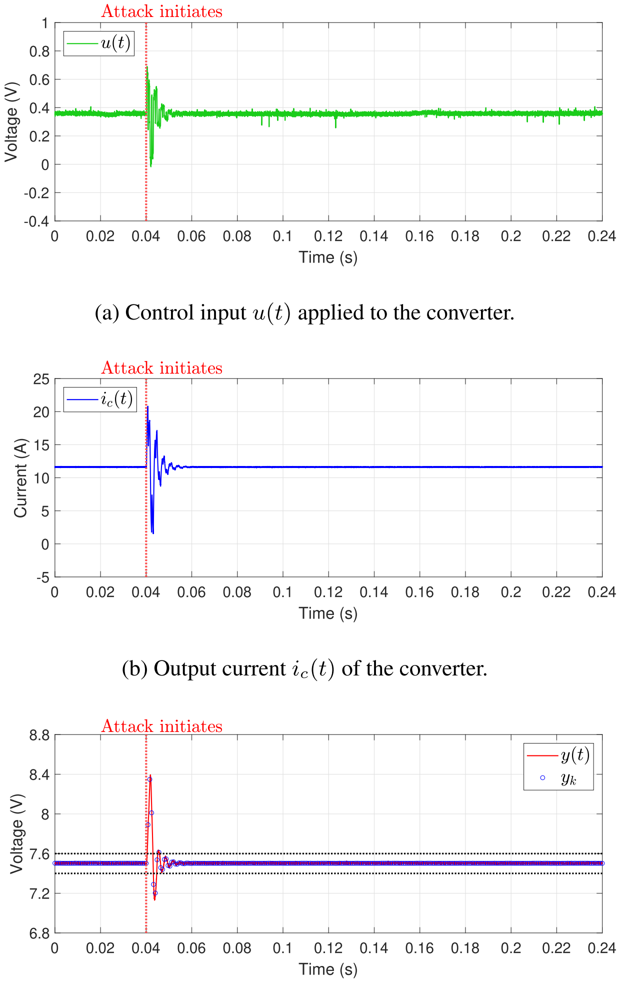


(a) Control input $u(t)$ applied to the converter.

(b) Output current $i_c(t)$ of the converter.

(c) Oscilloscope output (red line) and sensor output (blue circle).

FIGURE 12. System behavior under a stealthy attack: the system has zero-order hold in the input side and the zero-dynamics attack is constructed from *G*(*s*) with zero-order hold, i.e. from (15) or (17).



(a) Control input $u(t)$ applied to the converter.

(b) Output current $i_c(t)$ of the converter.

(c) Oscilloscope output (red line) and sensor output (blue circle).

FIGURE 13. Neutralization of zero-dynamics attack under generalized hold: zero-dynamics attack is constructed from *G*(*s*) with generalized hold whose zero-dynamics is stable and converges to zero.

is saturated and oscillates within the input constraint range (0 V to 0.75 V).

The output current of the converter $i_c(t)$ (see Fig. 5) measured with an oscilloscope is shown in Fig. 12b. Since the input applied to the converter oscillates under the effect of an attack, it can be seen that the output of the converter also oscillates in proportion.

Fig. 12c shows the system outputs $y(t)$ and y_k. The signal $y(t)$ is measured using an oscilloscope and can be regarded as the continuous-time signal, while y_k is measured every sampling period T_s using a voltage sensor. Due to the effect of ZDA, the continuous-time output $y(t)$ of the system oscillates over time, but the discrete-time output y_k does not exceed the threshold, so it is difficult to recognize that the system is under attack by remote monitoring.

B. SCENARIO 2

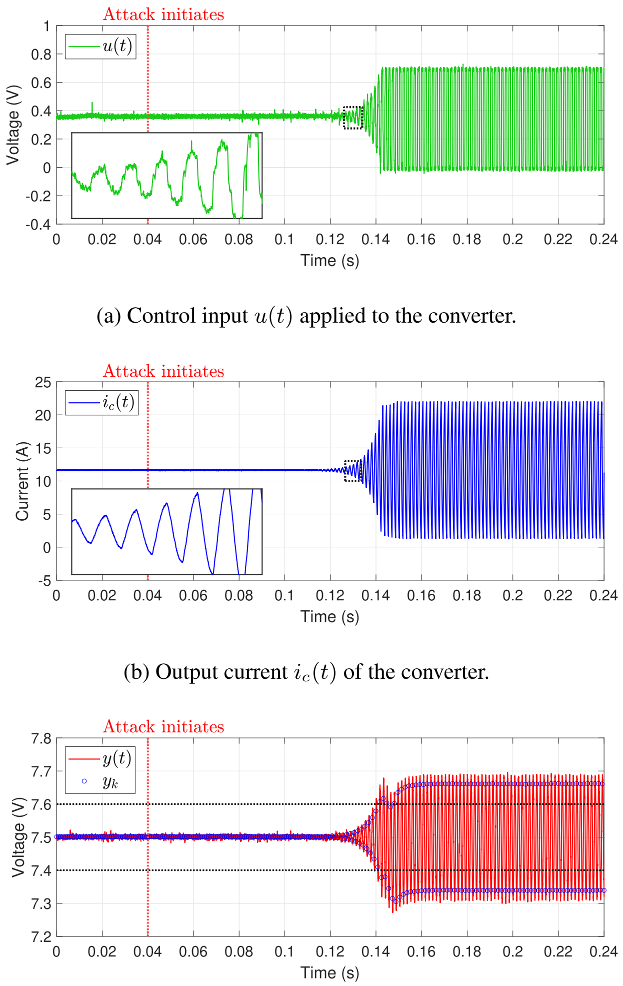
Suppose a GH, instead of ZOH, is used as a hold device. If the GH is designed so that the zero-dynamics of the new sampled-data system is stable, then the ZDA based on this new zero-dynamics converges to zero asymptotically, meaning that it has no or little effect on the system.

The hold gain h is set to (23) and $\zeta_0 = \begin{bmatrix}-0.858 & 0.515\end{bmatrix} \times 10^{-8}$. The attack is generated by using the zero-dynamics of the system with GH, and the parameters are given by $S_{\mathrm{d,GH}} = \begin{bmatrix}0 & 1\\ 0 & -0.6\end{bmatrix}$, $\psi_{\mathrm{d,GH}}^{\top} = \begin{bmatrix}3.53 \times 10^{-3} & -1.13\end{bmatrix}$, $g_{\mathrm{d,GH}} = 1.45 \times 10^{-9}$.

Fig. 13 shows the experimental result for this scenario. The initial condition ζ_0 is chosen similarly to Scenario 1, but the initial value of a_k is larger than Scenario 1 because the gain $\frac{1}{g_{\mathrm{d}}}$ is large so that the effect of ZDA appears immediately. However, the attack signal converges to zero eventually since the zero-dynamics is stable.

C. SCENARIO 3

In the last scenario, we consider the case where the attacker is unaware of the existence of GH and apply the ZDA that



(a) Control input $u(t)$ applied to the converter.

(b) Output current $i_c(t)$ of the converter.

(c) Oscilloscope output (red line) and sensor output (blue circle).

FIGURE 14. Detection of zero-dynamics attack: the attack is based on the unstable zero-dynamics considered in Scenario 1, while the actual zero-dynamics under generalized hold is stable.

is used in Scenario 1. If the system with GH has stable zero-dynamics, then the unstable attack will be clearly detected by monitoring the sampled output.

Fig. 14 demonstrates the detection of the unstable ZDA when GH is employed. The hold gain h for GH is chosen as (23), and the parameters for ZDA are the same as in Scenario 1. It is clearly seen that unlike Scenario 1, the sampled output y_k oscillates outside the threshold and hence the presence of attack can be detected by the monitoring system and actions to protect the system can be initiated.

VII. CONCLUSION

In this paper, we consider the security problem of DC-DC converter which is widely used in many applications. It is shown that even if the continuous-time system has stable zero-dynamics, the zero-dynamics of the sampled-data system can be unstable when ZOH is employed, which implies that the system is vulnerable to ZDA. The effect of ZDA is then demonstrated by simulations and experiments. In order to protect the system from ZDA, a countermeasure employing GH is introduced. Considering both situations where the attacker knows the presence of GH or not, it has been experimentally verified that this stealthy attack can be effectively neutralized or detected using GH. As a future research topic, we plan to study the zero assignment problem that is robust to system uncertainty. In addition, the study of defense techniques considering nonlinear systems will be an interesting research topic.

REFERENCES

[1] 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.

[2] V. L. Do, L. Fillatre, I. Nikiforov, and P. Willett, “Security of SCADA systems against cyber–physical attacks,” *IEEE Aerosp. Electron. Syst. Mag.*, vol. 32, no. 5, pp. 28–45, May 2017.

[3] J. P. Farwell and R. Rohozinski, “Stuxnet and the future of cyber war,” *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[4] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, “A review of cyber security risk assessment methods for SCADA systems,” *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2015.

[5] J. P. Conti, “The day the samba stopped [power blackouts],” *Eng. Technol.*, vol. 5, no. 4, pp. 46–47, Mar. 2010.

[6] R. M. Lee, M. J. Assante, and T. Conway, “Analysis of the cyber attack on the Ukrainian power grid,” Electr. Inf. Sharing Anal. Center (E-ISAC), Washington, DC, USA, 2016, vol. 388.

[7] K. H. LaCommare and J. H. Eto, “Understanding the cost of power interruptions to U.S. electricity consumers,” Lawrence Berkeley Nat. Lab. (LBNL), Berkeley, CA, USA, Tech. Rep. LBNL-55718, 2004.

[8] W. J. Broad, “Reports suggests problems with Iran’s nuclear effort,” New York Times, Nov. 2010.

[9] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 13, pp. 1–33, May 2011.

[10] H. Zhang, P. Cheng, L. Shi, and J. Chen, “Optimal DoS attack policy against remote state estimation,” in *Proc. 52nd IEEE Conf. Decis. Control*, Dec. 2013, pp. 5444–5449.

[11] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “Revealing stealthy attacks in control systems,” in *Proc. 50th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Oct. 2012, pp. 1806–1813.

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

[13] S. Weerakkody, X. Liu, and B. Sinopoli, “Robust structural analysis and design of distributed control systems to prevent zero dynamics attacks,” in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Dec. 2017, pp. 1356–1361.

[14] H. Jafarnejadsani, H. Lee, N. Hovakimyan, and P. Voulgaris, “A multirate adaptive control for MIMO systems with application to cyber-physical security,” in *Proc. IEEE Conf. Decis. Control (CDC)*, Dec. 2018, pp. 6620–6625.

[15] Y. Mao, E. Akyol, and Z. Zhang, “Strategic topology switching for security—Part II: Detection & switching topologies,” 2017, *arXiv:1711.11181*.

[16] Y. Mao, E. Akyol, and Z. Zhang, “A novel defense strategy against zero-dynamics attacks in multi-agent systems,” in *Proc. IEEE 58th Conf. Decis. Control (CDC)*, Dec. 2019, pp. 3563–3568.

[17] J. Lee, J. Kim, and H. Shim, “Zero-dynamics attack on homomorphically encrypted control system,” in *Proc. 20th Int. Conf. Control, Autom. Syst. (ICCAS)*, Oct. 2020, pp. 385–390.

[18] Y. Mao, H. Jafarnejadsani, P. Zhao, E. Akyol, and N. Hovakimyan, “Novel stealthy attack and defense strategies for networked control systems,” *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3847–3862, Sep. 2020.

[19] S. A. Pasha and A. Ayub, “Zero-dynamics attacks on networked control systems,” *J. Process Control*, vol. 105, pp. 99–107, Sep. 2021.

[20] H. Shim, J. Back, Y. Eun, G. Park, and J. Kim, “Zero-dynamics attack, variations, and countermeasures,” 2021, *arXiv:2101.00556*.

[21] G. Park, C. Lee, H. Shim, Y. Eun, and K. H. Johansson, "Stealthy adversaries against uncertain cyber-physical systems: Threat of robust zero-dynamics attack," *IEEE Trans. Autom. Control*, vol. 64, no. 12, pp. 4907–4919, Dec. 2019.

[22] G. Park, C. Lee, and H. Shim, "On stealthiness of zero-dynamics attacks against uncertain nonlinear systems: A case study with quadruple-tank process," in *Proc. Int. Symp. Math. Theory Netw. Syst.*, 2018, pp. 10–17.

[23] A. Hoehn and P. Zhang, "Detection of covert attacks and zero dynamics attacks in cyber-physical systems," in *Proc. Amer. Control Conf. (ACC)*, Jul. 2016, pp. 302–307.

[24] M. Naghnaeian, N. Hirzallah, and P. G. Voulgaris, "Dual rate control for security in cyber-physical systems," in *Proc. 54th IEEE Conf. Decis. Control (CDC)*, Dec. 2015, pp. 1415–1420.

[25] J. I. Yuz and G. C. Goodwin, *Sampled-Data Models for Linear and Nonlinear Systems*. London, U.K.: Springer, 2014.

[26] J. Kim, J. Back, G. Park, C. Lee, H. Shim, and P. G. Voulgaris, "Neutralizing zero dynamics attack on sampled-data systems via generalized holds," *Automatica*, vol. 113, Mar. 2020, Art. no. 108778.

[27] D. Kim, K. Ryu, J. H. Kim, and J. Back, "Zero assignment via generalized sampler: A countermeasure against zero-dynamics attack," *IEEE Access*, vol. 9, pp. 109932–109942, 2021.

[28] D. Kim, K. Ryu, and J. Back, "Zero-dynamics attack on wind turbines and countermeasures using generalized hold and generalized sampler," *Appl. Sci.*, vol. 11, no. 3, p. 1257, Jan. 2021.

[29] 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.*, 2012, pp. 55–64.

[30] S. Sahoo, S. Mishra, J. C. Peng, and T. Dragičević, "A stealth cyber-attack detection strategy for DC microgrids," *IEEE Trans. Power Electron.*, vol. 34, no. 8, pp. 8162–8174, Aug. 2018.

[31] W. Li, X. Zhang, and H. Li, "Co-simulation platforms for co-design of networked control systems: An overview," *Control Eng. Pract.*, vol. 23, pp. 44–56, Feb. 2014.

[32] R. Yang, Y. Yu, J. Sun, and H. R. Karimi, "Event-based networked predictive control for networked control systems subject to two-channel delays," *Inf. Sci.*, vol. 524, pp. 136–147, Jul. 2020.

[33] Q. Shafiee, S. Member, J. M. Guerrero, S. Member, and J. C. Vasquez, "Distributed secondary control for islanded microgrids—A novel approach," *IEEE Trans. Power Electron.*, vol. 29, no. 2, pp. 1018–1031, Feb. 2014.

[34] H. K. Khalil, *Nonlinear Systems*, vol. 3. Upper Saddle River, NJ, USA: Prentice-Hall, 2002.

[35] P. Kabamba, "Control of linear systems using generalized sampled-data hold functions," *IEEE Trans. Autom. Control*, vol. AC-32, no. 9, pp. 772–783, Sep. 1987.

[36] J. Back, J. Kim, C. Lee, G. Park, and H. Shim, "Enhancement of security against zero dynamics attack via generalized hold," in *Proc. IEEE 56th Annu. Conf. Decis. Control (CDC)*, Dec. 2017, pp. 1350–1355.

[37] H. He, R. Xiong, and J. Fan, "Evaluation of lithium-ion battery equivalent circuit models for state of charge estimation by an experimental approach," *Energies*, vol. 4, no. 4, pp. 582–598, Mar. 2011.

BUMSU KIM (Graduate Student Member, IEEE) received the B.S. degree from the Department of Electronic Engineering, Hankyong National University, in 2017. He is currently pursuing the Ph.D. degree with the School of Robotics, Kwangwoon University. His research interests include security and multi-agent systems.

KUNHEE RYU (Graduate Student Member, IEEE) received the B.S. and M.S. degrees in control and instruments engineering from Kwangwoon University, in 2012 and 2014, respectively, where he is currently pursuing the Ph.D. degree with the School of Robotics. His research interests include robotics and distributed systems.

JUHOON BACK (Member, IEEE) received the B.S. and M.S. degrees in mechanical design and production engineering and the Ph.D. degree from the School of Electrical Engineering and Computer Science, Seoul National University, Seoul, South Korea, in 1997, 1999, and 2004, respectively. From 2005 to 2006, he worked as a Research Associate at the Control and Power Group, Electrical and Electronic Engineering, Imperial College London, U.K. He is currently a Professor with the School of Robotics, Kwangwoon University, Seoul. His research interests include nonlinear control, estimation, multi-agent systems, and their applications to renewable energy systems, vehicle control systems, and robotics. He is an Associate Editor of the *Systems and Control Letters* and IEEE CONTROL SYSTEMS LETTERS.