Cyber-Physical Secure Observer-Based Corrective Control under Compromised Sensor Measurements

Dan Wu, Pallavi Bharadwaj, Premila Rowles, and Marija Ilić

***Abstract*— In this paper we introduce the objectives and design principles of corrective control under cyber-physical attacks. We propose two types of observer-based corrective control for both the open-loop stable and the open-loop unstable LTI systems. The basic idea of our corrective control design is to use the observer as the ground-truth during the attack, making the plant dynamics follow the observer behavior. This is the opposite to the no-attack-detected period in which the observer is designed to follow the plant dynamics. We show stability of the proposed control under compromised sensor measurements, and quantify the effects of the discrepancy between the observer and the plant. Numerical examples, with illustrations using microgrid energy dynamics, are presented to show benefits of the proposed corrective control.**

cyber-physical security, corrective control, observer, deception attack; cyber-secure micro-grids

I. Introduction

The advancement of communication technologies has enabled a deep merge of the information layer with the physical layer in today's man-made systems through embedded distributed devices. In order to control the cost for large-scale implementations, these devices usually have low communication and computation capacities, making them very vulnerable to cyber-physical attacks [1]. Their parts are produced and assembled from different factories all over the world, making the end users further difficult to trace and check their security in advance. In recent years, cyber-physical security problems become more prominent, some of which have caused severe damages to the society.

Cyber-physical attacks can be roughly grouped into two categories: the denial of service (DoS) attack and the deception attack. The DoS attack aims at blocking or postponing communication among different physical components in order to degrade the performance, or event destabilize the system [2], [3]. The deception attack aims at destabilize the system by injecting false data, compromised sensor measurements, or malicious control commands [1], [4].

To ensure cyber-physical security from these attacks, many defensive strategies have been proposed, including attack detection schemes [5]–[9], secure state estimation strategies [10]–[14], control consensus designs [1], [15], and security controls [1], [16]–[18].

The secure state estimation is the core step for further security control of the system after the identification of an attack. While the Kalman filter technique has been used for decays to estimate system states [19], recently the observer-based methods acquired more attention. Under sparse attack assumptions, [20] showed that a system requires a certain amount of uncorrupted sensors, at least two times the number of the corrupted sensors, to remain resilient against sensor attacks. Finding those uncorrupted sensor locations is a combinatorial problem [5], which can be solved by either brutal force search [13], [16] or optimization methods [21]. However, these methods usually depend on strong computation capability for finding the available distributed observers, and rely on intensive communications. Thus, they may not be suitable for quick-response required circumstances.

To tackle the situation when secure state estimation is not available but prompt actions are required to regulate the system behavior under attacks, in this paper we propose cyber-physical secure observer-based corrective control methods. The basic idea is to use the observer as the ground-truth during the attack, making the plant dynamics follow the observer behavior. The approach can completely reject any compromised sensor measurements for the open-loop stable LTI system, and can maintain the intact observer subsystem needed to establish a credible desired system behavior reference for the open-loop unstable system. The major contributions are summarized below.

1) We proposed the basic design principles for the cyber-physical secure corrective control under sensor attacks.
2) We proposed an innovative framework to use the Luenberger observer as a ground-truth to correct the system behavior during sensor attacks.
3) We proposed the blind corrective control scheme for open-loop stable LTI systems to defend against sensor attacks, and showed asymptotic stability under the finite attack energy assumption.
4) We proposed the switch-role corrective control scheme for open-loop unstable LTI systems to defend against sensor attacks and showed the input-to-state stability.

II. Problem Formulation

A. Plant Dynamics

We consider our target plant as a continuous linear time-invariant dynamical system given below.

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

$$y(t) = Cx(t) \tag{2}$$

where $A \in \mathbb{R}^{n\times n}$ is the open-loop matrix of the plant, $B \in \mathbb{R}^{n\times p}$ is the control matrix, $C \in \mathbb{R}^{m\times n}$ is the output matrix; $x(t) \in \mathbb{R}^n$ is the state variable vector of the plant, $u(t) \in \mathbb{R}^p$

Laboratory for Information and Decision Systems, Massachusetts Institute of Technology, Cambridge, MA, danwumit@mit.edu, bpallavi@mit.edu, premila@mit.edu, ilic@mit.edu

is the control vector, $d(t) \in \mathbb{R}^n$ is the external disturbance vector, $y(t) \in \mathbb{R}^m$ is the output vector of the plant, which will be used in the observer shortly below.

We further assume that (A, B) is controllable, (A, C) is observable, and the total energy of the disturbance $d(t)$ is finite, i.e., $\int_0^\infty d(t)^T d(t) dt < +\infty$, so that the disturbance will eventually be damped out by the closed-loop system. This is an ideal assumption for asymptotic stability. In practice, systems nonetheless experience certain random noises. As long as the noise is bounded, the closed-loop asymptotic stable LTI system yields a bounded output.

B. Observer Setup

To estimate the states of system (1), we consider the Luenberger observer as follow.

$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + Bu(t) + L\big(y(t) - C\hat{x}(t)\big) \tag{3}$$

where $\hat{A} \in \mathbb{R}^{n\times n}$ is an estimation of the open-loop matrix A of the plant, $\hat{x}(t) \in \mathbb{R}^n$ is the state variable vector of the observer, which is regarded as an estimate of the true state variable $x(t)$, $L \in \mathbb{R}^{n\times m}$ is the observer gain matrix which is designed to make $\hat{x}(t)$ quickly follow up the true state variable $x(t)$, typically $10\times$ faster than system (1). **Note:** The observer open-loop matrix $\hat{A}$ is usually assumed to be the same as the plant open-loop matrix A. In practice, however, it is difficult to match $\hat{A}$ with A exactly due to some nonlinearity of the plant system, measurement errors, etc. We will discuss the influence of this mismatch later in Section III-E to quantify its influence on our corrective control designs. The observer state variable $\hat{x}(t)$ is used to design the feedback controller for both the observer system (3) and the plant system (1).

$$u(t) = K\hat{x}(t) - r(t) \tag{4}$$

where $K \in \mathbb{R}^{m\times n}$ is the control gain matrix designed to allocate the poles of the plant, $r(t) \in \mathbb{R}^n$ is an external reference command which comes from a higher layer control scheme with a slower time-scale. This is typical in many engineering designs, for example, the automatic generation control (AGC) in power systems. We will discuss this reference command signal $r(t)$ shortly below.

C. Adversary Attack Model

Throughout this paper, we consider the active adversary who is capable of altering the measurement from the sensors and launching the deception attack.

In (2), instead of having an exact measurement $y(t)$, we have a compromised measurement $\tilde{y}(t)$ such that

$$\tilde{y}(t) = Cx(t) + \omega(t) \tag{5}$$

where $\omega(t) \in \mathbb{R}^m$ is the deception attack signal that has been conspired and injected into the sensor. Therefore, the observer model (3) becomes

$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + Bu(t) + L\big(\tilde{y}(t) - C\hat{x}(t)\big) \tag{6}$$

We assume that: i) The deception attack signal $\omega(t)$ can be detected; ii) The observer is intact; and, iii) The external reference command signal $r(t)$ is authentic. The first assumption is based on numerous existing work which devotes to identifying the existence of attack signals, for example, the dynamic watermarking technique [7], [22], [23] actively injects a credential signal to the system and monitor the change of its statistic behavior to identify attacks. The second assumption suggests that the parameters of the observer system cannot be altered by the adversary. Our corrective control designs will largely rely on this assumption. The third assumption differentiates attacks on different control layers, and brings our attention to the primary control layer only.

D. Corrective Control Objective

Our corrective control objective is to answer the following question: *Given an authentic external reference command $r(t)$, if the sensor measurements $y(t)$ are compromised by a deception attack $\omega(t)$, and the attack has been successfully detected, can we design a corrective scheme to retain the objective of the higher layer control command $r(t)$.*

In another word, we hope the external reference command $r(t)$ in (4) is still functioning in the compromised system, and guide the corrective controller to yield the desired (maybe degraded) outcome. For example, without any corrective control designs, a generator's output power can continuously deviate away from its dispatch value by a deception attack. While with some corrective scheme, the generator's output only temporarily deviates away from its dispatch value.

Note: A corrective controller is considered as an acting (or backup) controller to replace the original one for a temporary use only. One should never regard it as a full functioning controller, nor expect it to achieve the same performance. Otherwise, a duplicate original controller would serve the purpose. For example in our circumstances, if a sensor has been compromised, the most straightforward way is to replace it with a duplicate sensor, provided the duplicate sensor has been installed in advance.

The design principles of the corrective controller should follow the following principles:

1) A corrective controller should be anchored to some ground-truth information which can hardly be tampered by the adversary. This is where "correction" comes from.
2) A corrective controller should make a compromise among cost, complexity, and performance. It should be cheap to install (comparing to a duplicate original controller), easy to apply and operate (less dependent on frequent communications and heavy computations), and able to achieve certain temporary control performance.
3) A corrective controller should be effective for a broad range of attack forms, rather than a specific attack form.

III. Observer-Based Corrective Control Design

A. Ground-Truth Information

According to our control objective, given a detected attack, the controller should "correct" the system behavior to (partially) retain its primary goal. This correction must refer to some ground-truth.

Recall the observer (6) and the plant (1), despite the difference between $\hat{A}$ and A, the observer can be regarded as a replica of the original plant. If no attack happens, it achieves the same desired state associated with the external reference command $r(t)$.

The basic idea of our corrective control design is to use the observer as a ground-truth during the attack, making the plant dynamics follow the observer's behavior. This is the opposite to the no-attack-detected period in which the observer is designed to follow the plant dynamics.

B. Blind Corrective Control

If we assume that the open-loop system is stable, then we design the corrective controller as follow.

$$\dot{x}(t) = Ax(t) + Bu(t) + d(t) \tag{7a}$$
$$\tilde{y}(t) = Cx(t) + \omega(t) \tag{7b}$$
$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + Bu(t) + L(t)\big(\tilde{y}(t) - C\hat{x}(t)\big) \tag{7c}$$
$$u(t) = K\hat{x}(t) - r(t) \tag{7d}$$

where

$$L(t) = \begin{cases} 0, & \text{if } \omega(t) \text{ is detected} \\ L, & \text{otherwise} \end{cases} \tag{8}$$

When $\omega(t)$ is detected, the overall system is

$$\dot{x}(t) = Ax(t) + Bu(t) + d(t) \tag{9a}$$
$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + Bu(t) \tag{9b}$$

The first advantage comes from the fact that (9) is completely quarantined from the compromised measurement $\tilde{y}(t)$, thus, will never be influenced by the attack $\omega(t)$.

Let's further assume that $\hat{A} = A$, then the error $e(t) := x(t) - \hat{x}(t)$ is given below.

$$\dot{e}(t) = Ae(t) + d(t) \tag{10}$$

Since A is a stable matrix by our assumption, the error $e(t)$ will converge to zero in the asymptotic sense with finite energy $d(t)$. Comparing to the no-attack-detected case, the error converges much slower in (10) because the observer is "blind" of any external disturbance $d(t)$, which gives the name "blind corrective control". It is the compromise we have to make for keeping the observer intact while rejecting any attacks on the sensor measurements.

The second advantage of (7) is that it can still follow the instruction from the external reference command $r(t)$. A naive way of disabling the control matrix B can also reject any sensor attacks, but it rejects external reference command as well.

C. Switch-Role Corrective Control

In the case when the open-loop system is unstable, the blind corrective control may lose stability. Therefore, we provide another corrective control design below.

$$\dot{x}(t) = Ax(t) + Bu(t) + L_p\big(C\hat{x}(t) - \tilde{y}(t)\big) + d(t) \tag{11a}$$
$$\tilde{y}(t) = Cx(t) + \omega(t) \tag{11b}$$
$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + Bu(t) + L\big(\tilde{y}(t) - C\hat{x}(t)\big) \tag{11c}$$
$$u(t) = K\hat{x}(t) - r(t) \tag{11d}$$

where

$$L_p = \begin{cases} L_p, & \text{if } \omega(t) \text{ is detected} \\ 0, & \text{otherwise} \end{cases} \tag{12a}$$
$$L = \begin{cases} 0, & \text{if } \omega(t) \text{ is detected} \\ L, & \text{otherwise} \end{cases} \tag{12b}$$

When $\omega(t)$ is detected, the overall system is

$$\dot{x}(t) = Ax(t) + Bu(t) + L_p\big(C\hat{x}(t) - \tilde{y}(t)\big) + d(t) \tag{13a}$$
$$\dot{\hat{x}}(t) = \hat{A}\hat{x}(t) + Bu(t) \tag{13b}$$

A first glance at (13) reminds people of a standard observer-based control system, but with a flipped structure. The plant system looks like an observer, while the observer system looks like a plant. This is why we call it "switch-role corrective control". The main purpose of this design is to ask the plant to follow the observer during the attack.

One may notice that in this case we are no longer able to completely reject the attack signal $\omega(t)$ since in (13a) the tampered measurement $\tilde{y}(t)$ still exists. Then, the question is, what's the benefit of doing this? Recall that if no corrective control during an attack, the measurement $\tilde{y}(t)$ brings the attack signal $\omega(t)$ to the observer system (6), compromising the control signal $u(t)$. This $u(t)$, in return, enters the plant system (1), polluting the plant dynamics. During this process, neither the plant nor the observer remains credible. With the switch-role corrective control, the observer system (13b) rejects the attack signal $\omega(t)$ and remains intact, which naturally serves as a ground-truth to guide the plant system.

If we assume that $\hat{A} = A$, the error $e(t) := \hat{x}(t) - x(t)$ dynamics is

$$\dot{e}(t) = (A - L_pC)e(t) + L_p\omega(t) + d(t) \tag{14}$$

Although A is an unstable matrix, the error can still vanish to zero in the asymptotic sense, provided a good design of L_p and $\omega(t) = 0$.

D. Stability Analysis

For the blind corrective control design, we show the following result.

Theorem 1. *For a given observer-based control system* (7) *with the control design* (8)*, if it is open-loop stable with $\hat{A} = A$, and $\omega(t)$ is detected, the associated control system* (9) *is globally asymptotically stable under finite energy disturbance $d(t)$.*

Proof: Note that the observer subsystem (9b) is a stand-alone globally asymptotically stable system. We need to show the plant subsystem (9a) is also globally asymptotically stable.

Recall (10), since A is a stable matrix, the natural response of the error state $e(t)$ is asymptotically stable. On the other hand, we have finite energy disturbance $d(t)$ which implies that for any $\epsilon > 0$, there exists a finite time T such that for any $t > T$, $\int_t^\infty |d(t)| < \epsilon$. Hence, for any initial error $e(0)$ and any $\delta > 0$, we can always find a time $T^\star$ such that for any $t > T^\star$, $|e(t)| < \delta$. It suggests that the error system is globally asymptotically stable.

Finally, the plant state $x(t) = \hat{x}(t) + e(t)$, which is also globally asymptotically stable.

For the switch-role corrective control design, since the attack signal $\omega(t)$ is not necessarily assumed to have finite energy, we show the input-to-state stability [24].

Definition 1 ($\mathcal{K}$ function)**.** A function $\gamma : \mathbb{R}_+ \to \mathbb{R}_+$ is in the $\mathcal{K}$ class if it is continuous, strictly increasing, unbounded, and $\gamma(0) = 0$.

Definition 2 ($\mathcal{KL}$ function)**.** A function $\beta : \mathbb{R}_+^2 \to \mathbb{R}_+$ is in the $\mathcal{KL}$ class if $\beta(\cdot, t) \in \mathcal{K}$ for any t, and $\beta(x, t) \to 0$ as $t \to \infty$.

Definition 3 (input-to-state stability)**.** Consider a dynamical system with the state variable $x(t)$ and the external input $s(t)$, if there exist some function $\beta \in \mathcal{KL}$ and $\gamma \in \mathcal{K}$ such that

$$||x(t)||_2 \leq \beta(||x_0||_2, t) + \gamma(||s(t)||_\infty)$$

then we say the system is input-to-state stable.

Theorem 2. *For a given observer-based control system* (11) *with the control design* (12)*, if $\hat{A} = A$, and $\omega(t)$ is detected, then the associated control system* (13) *is input-to-state stable.*

Proof: System (13) can be expressed as follow.

$$\dot{z}(t) = A_c z(t) + B_c s(t) \tag{15}$$

where $z(t)$ includes $x(t)$ and $\hat{x}(t)$, $s(t)$ includes $\omega(t)$, $r(t)$, and $d(t)$, and

$$A_c = \begin{bmatrix} A - L_p C & BK + L_p C \\ 0 & A + BK \end{bmatrix}$$
$$B_c = \begin{bmatrix} -L_p & -B & I & 0 \\ 0 & -B & 0 & I \end{bmatrix}$$

If $s(t) = 0$, by the argument in the proof of Theorem 1 system (15) is globally asymptotically stable, which implies that A_c is stable. Hence, we have $||e^{A_c t}||_2 \leq Ne^{-\lambda t}$ for some $N > 0$ and $\lambda > 0$. Then,

$$\begin{aligned} ||z(t)||_2 &= ||e^{A_c t} z_0 + \int_0^t e^{A_c(t-\tau)} B_c s(\tau) d\tau||_2 \\ &\leq Ne^{-\lambda t}||z_0||_2 + ||B_c||N \int_0^t e^{-\lambda(t-\tau)} d\tau ||s||_\infty \\ &= Ne^{-\lambda t}||z_0||_2 + ||B_c||\frac{N}{\lambda}(1 - e^{-\lambda t})||s||_\infty \\ &\leq Ne^{-\lambda t}||z_0||_2 + ||B_c||\frac{N}{\lambda}||s||_\infty \end{aligned}$$

Let $\beta = Ne^{-\lambda t}||z_0||_2$ and $\gamma = ||B_c||\frac{N}{\lambda}||s||_\infty$, we have $\beta \in \mathcal{KL}$ and $\gamma \in \mathcal{K}$, which complete the proof.

E. Observer Fidelity under Variations

Our corrective controls rely on the fidelity of the observer as the ground-truth to guide the behavior of the plant under attack. In reality, the observer open-loop matrix $\hat{A}$ may not be the same as the plant open-loop matrix A. Therefore, we need to quantify the effect of this discrepancy.

Suppose $\hat{A} = A + \delta A$, where $\delta A \in \mathbb{R}^{n \times n}$ is a small variation from A. During an attack, we have.

$$\hat{x}_\infty^{ex} = A_{bk}^{-1} Br \tag{17a}$$
$$\hat{x}_\infty^{var} = (A_{bk} + \delta A)^{-1} Br \tag{17b}$$

where $\hat{x}_\infty^{ex}$ is the steady state of the observer with exact A, $\hat{x}_\infty^{var}$ is the steady state of the observer with a variation $A + \delta A$, $A_{bk} = A + BK$. Now let's quantify the difference between $\hat{x}_\infty^{ex}$ and $\hat{x}_\infty^{var}$ with respect to δA.

Theorem 3. *Suppose the external reference command r is constant and non-zero, $I + A_{bk}^{-1}\delta A$ is invertible, then the difference $d\hat{x}$ between $\hat{x}_\infty^{ex}$ and $\hat{x}_\infty^{var}$ satisfies*

$$\frac{||d\hat{x}||}{||r||} \leq \frac{\sigma_m}{\sigma_m - \sigma_a} \frac{\sigma_a}{\sigma_m^2} \sigma_b \tag{18}$$

where σ_m is the smallest singular value of A_{bk}, σ_a is the largest singular value of δA, σ_b is the largest singular value of B.

Proof: By [25] and $I + A_{bk}^{-1}\delta A$ being invertible,

$$\begin{aligned} \hat{x}_\infty^{var} &= (A_{bk} + \delta A)^{-1} Br \\ &= A_{bk}^{-1} Br - (I + A_{bk}^{-1}\delta A)^{-1} A_{bk}^{-1}(\delta A) A_{bk}^{-1} Br \end{aligned}$$

Thus, we have

$$\begin{aligned} \frac{||d\hat{x}||}{||r||} &= \frac{||(I + A_{bk}^{-1}\delta A)^{-1} A_{bk}^{-1}(\delta A) A_{bk}^{-1} Br||}{||r||} \\ &\leq ||(I + A_{bk}^{-1}\delta A)^{-1}|| ||A_{bk}^{-1}||^2 ||\delta A|| ||B|| \\ &\leq \frac{\sigma_m}{\sigma_m - \sigma_a} \frac{\sigma_a}{\sigma_m^2} \sigma_b \end{aligned}$$

which concludes the proof.

Note that if δA is small enough, σ_a is close to zero, which yields a small bound on $d\hat{x}$, suggesting good fidelity of the observer. On the other hand, if δA is large enough, σ_a approaches σ_m, which drives $\frac{\sigma_m}{\sigma_m - \sigma_a}$ to infinity, creating a large error bound on the final state of the observer.

In practical engineering, many systems can exhibit nonlinearity at different operating points, which can increase the discrepancy between a pre-determined observer and the plant. Using system identification techniques or other learning-based methods can reduce this discrepancy.

IV. Numerical Demonstrations

A. Numerical Settings

For the blind corrective control experiment, we consider the following open-loop stable System-1.

$$A = \begin{bmatrix} -0.5 & 0.2 & 0.2 \\ -0.1 & -0.5 & 0 \\ 1 & 0 & -1 \end{bmatrix}, \; L = \begin{bmatrix} 9.5 & -1.875 & -1.875 \\ 0.2 & 8.25 & -0.75 \\ 0.2 & -0.75 & 18.25 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 \\ -1 & 0 \\ 0 & 1 \end{bmatrix}, \; C = I, \; K = \begin{bmatrix} 1.775 & 1.25 & 0.75 \\ -2.875 & -0.75 & -0.75 \end{bmatrix}$$

$$r(t) = \begin{cases} [2.525, -3.625]^T, & t \leq 50 \\ [3.6625, -5.0625]^T, & t > 50 \end{cases}$$

$$\omega(t) = [0.4, 0.3, 0.4]^T \times \delta(0.5t + 10), \; t = 0, 1, 2, \cdots$$

For the switch-role corrective control experiment, we consider the following open-loop unstable System-2.

$$A = \begin{bmatrix} 0.5 & 0.2 & 0.2 \\ -0.1 & -0.5 & 0 \\ 1 & 0 & -1 \end{bmatrix}, \; L = \begin{bmatrix} 10.5 & -9.375 & -9.375 \\ 0.2 & 7.75 & -1.25 \\ 0.2 & -1.25 & 17.75 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 \\ -1 & 0 \\ 0 & 1 \end{bmatrix}, \; L_p = \begin{bmatrix} 20.5 & -0.1 & 1 \\ 0.2 & 19.5 & 0 \\ 0.2 & 0 & 39 \end{bmatrix}$$

$$C = I, \; K = \begin{bmatrix} 9.275 & 1.75 & 1.25 \\ -10.375 & -1.25 & -1.25 \end{bmatrix}$$

$$r(t) = \begin{cases} [10.525, -11.625]^T, & t \leq 50 \\ [15.4125, 16.8125]^T, & t > 50 \end{cases}$$

$$\omega(t) = [0.4, 0.3, 0.4]^T \times \delta(0.5t + 10), \; t = 0, 1, 2, \cdots$$

B. Blind Corrective Control Performance

In this experiment, we consider the open-loop stable System-1 provided above. The external reference command $r(t)$ will change to a new value at 50 sec. The attack $\omega(t)$ is launched at 10 sec with a repeated impulse signal every 0.5 seconds.

In Fig. 1, no attack is launched. System-1 stabilizes quickly to a new equilibrium point when the external reference command changes at $t = 50$ sec.

In Fig. 2, System-1 is under attack but not corrective control reacts. The attack signal creates oscillations to the system and makes both the plant and observer states deviate away from the desired equilibrium point, comparing to Fig. 1.

In Fig. 3, the proposed blind corrective control is initiated after the attack was launched, with an assumed time delay of 10 seconds (This delay depends on how fast the attack can be detected). The plot shows that the blind corrective control completely rejects the attack signal, and brings both the plant and observer states back to the desired equilibrium point.

In Fig. 4, we consider the same experiment setting as in Fig. 3 except that we impose a small variation matrix δA on the observer matrix. We randomly choose δA which satisfies the condition $|\frac{\sigma_a}{\sigma_m}| \leq 5\%$. From the plot one can see that the observer and the plant converge to two slightly different equilibrium points. The difference of these equilibrium points is bounded by Theorem 3.

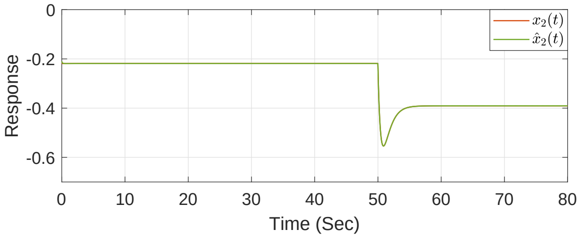

Fig. 1: System-1: No Attack

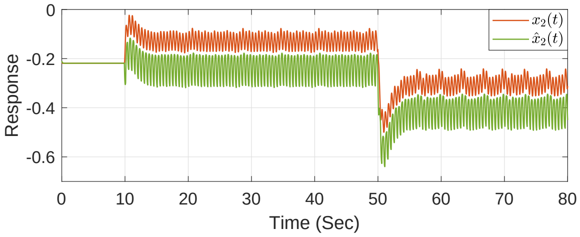

Fig. 2: System-1: under Attack without Corrective Control

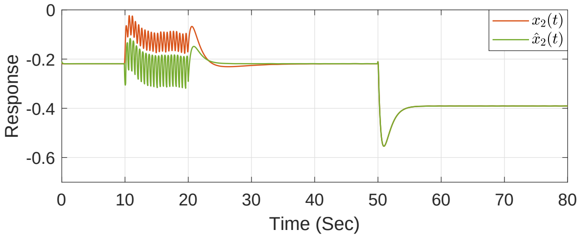

Fig. 3: System-1: under Attack with Blind Corrective Control

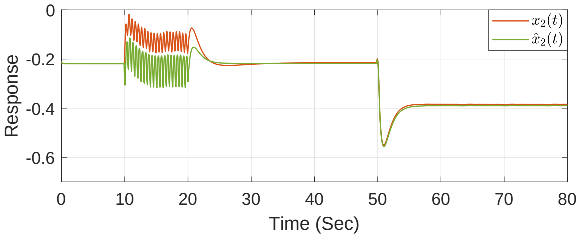

Fig. 4: System-1 with Observer Variation: under Attack with Blind Corrective Control

C. Switch-Role Corrective Control Performance

In this experiment, we consider the open-loop unstable System-2. The external reference command $r(t)$ will change to a new value at 50 sec. The attack $\omega(t)$ is launched at 10 sec with a repeated impulse signal every 0.5 seconds.

In Fig. 5, no attack is launched. System-2 stabilizes quickly to a new equilibrium point when the external reference command changes at $t = 50$ sec.

In Fig. 6, System-2 is under attack but not corrective control reacts. One can see that the attack signal creates oscillations to the system and makes both the plant and observer states deviate away from the desired equilibrium point, comparing to Fig. 5.

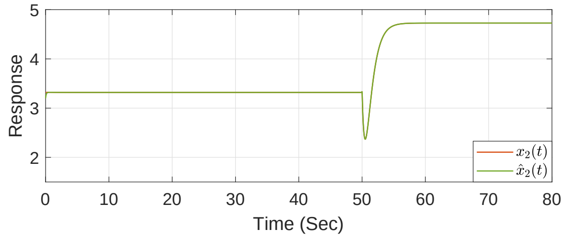

Fig. 5: System-2: No Attack

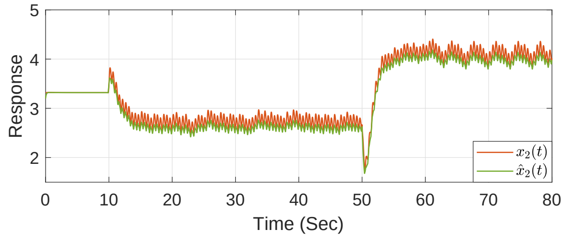

Fig. 6: System-2: under Attack without Corrective Control

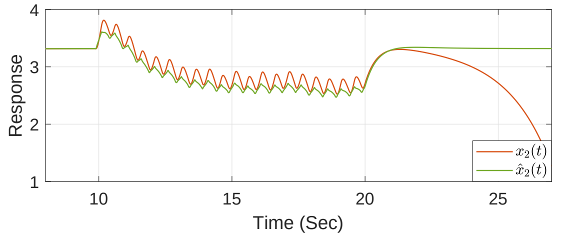

Fig. 7: System-2: under Attack with Blind Corrective Control

In Fig. 7, we launch the blind corrective control to System-2 under attack. As we discussed in Section III-B, the open-loop unstable system may lose stability with the blind corrective control. As expected, the plant state blows up shortly after the blind corrective control initiated in the plot.

In Fig. 8, the proposed switch-role corrective control is initiated after the attack was launched, with an assumed time delay of 10 seconds. The plot shows that the switch-role corrective control brings the observer state back to the desired equilibrium point, and forces the plant state to follow the observer state with a reduced oscillation amplitude when comparing to Fig. 6. It verifies the argument in Section III-C that the switch-role corrective control preserves the intactness of the observer, and attempts to regulate the plant state based on the observer behavior.

In Fig. 9, we consider the same experiment setting as in Fig. 8 except that we impose a small variation matrix δA on the observer matrix. We randomly choose δA which satisfies the condition $|\frac{\sigma_a}{\sigma_m}| \leq 5\%$. The influence of this variation is bounded by Theorem 3.

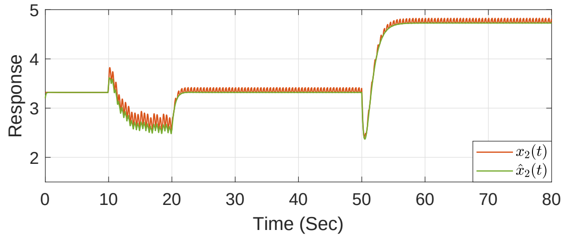

Fig. 8: System-2: under Attack with Switch-Role Corrective Control

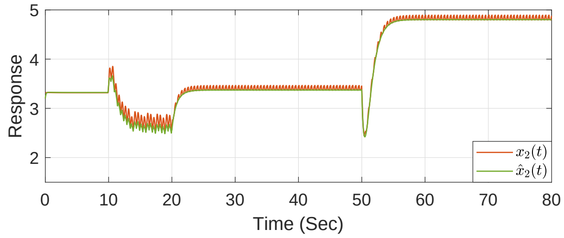

Fig. 9: System-2 with Observer Variation: under Attack with Switch-Role Corrective Control

V. Corrective Control for Microgrids

In this section we consider a real-world application of the proposed corrective control to make microgrids cyber-secure. A block diagram representation of a microgrid [26] is shown in Fig. 10. In Fig. 10 a three-phase inverter interfaces a photovoltaic (PV) voltage source to a three-phase ac load via LCL filters. The control architecture shown in this figure is based on the droop-based power control [26], wherein based on the output voltage and current measurements, real power and reactive power are calculated. The real power is linearly related with system frequency using a synthetic droop equation which is utilized to compute inverter voltage angle (integral of frequency). Reactive power and voltage are also related through a synthetic droop equation which ensures reactive power sharing in a microgrid within parallel inverters. This reactive power droop equation is used to provide voltage reference to the voltage controller which further compares reference value to the measured value and passes the error though a PI controller to further generate current reference for the inner current loop. The current controller compares the reference inverter current to the measured value and then passes the error to a faster PI controller which further generates the control voltage references which when

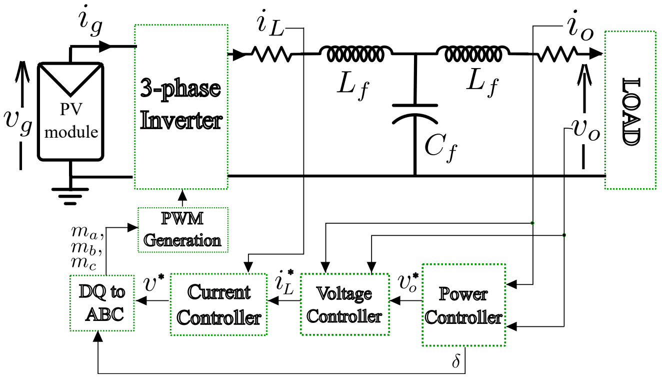

Fig. 10: A solar PV microgrid connected to its local load with a 3-phase inveterter and a LCL filter.

converted to 3-phase abc domain from dq domain are called inverter's modulating signals. These modulating signals are passed through the PWM generator which gives a high or low pulse to the inverter switches to turn them on or of, respectively.

Under deception attack on the microgrid [23] it is possible that the measurement sensors of the output voltage and currents can get tampered and the system control may go unstable as real measurements are concealed. In such a case, the proposed observer will come into action once the attack is detected [7]. As the controller is then based on the observer predicted system states, stability can again be ensured in the microgrid. Depending on the structure of the microgrid, complete mathematical formulation can be given based on the proposed approach. For the single PV source based 3-phase microgrid, states of the system are the filter inductor currents i_L, i_o and filter capacitor voltage v_c, $x = [i_L \ v_c \ i_o]$. The output of the system is the load voltage and current v_o and i_o, $[v_o \ i_o]$. The system control are the control voltage signals v_d, v_q in dq domain, $u = [v_{dq}]$, or the modulating signals m_a, m_b, m_c in the abc domain, respectively. So the entire system can be modelled in a linearized way [23].

A. *Modeling Observer of Energy Dynamics*

Notice that, strictly speaking, there is a switching nonlinearity introduced by the PWM implementation of microgrid control, but under the common assumption that LCL filter will smooth out the output the model is LTI and the theoretical results introduced in this paper are directly applicable. However, when the PWM switching is model, the switch leads to a bilinear model in which u is the switch position [27]. In order to overcome this nonlinearity, we consider a two-level energy model summarized next. Moreover, it can be seen from Fig. 10 that closed-loop microgrid dynamics can be quite complicated with multi-layer control. In such a case, a multi-layered modeling approach is introduced: the lower level is modeled in conventional state-space, and the higher layer model uses aggregate energy variables [28]. Notably, complex dynamic interactions within the aggregate model of the system are technology-agnostic and take on the standard state space form given in Equation (2). This model is expressed in terms of aggregate state variables stored energy E, rate of change of stored energy p and energy stored in tangent space E_t and are used to model the higher level interactions of microgrid with the rest of the system. The state space energy model is given as follows (19):

$$\dot{E} = P - E/\tau = p \tag{19}$$

$$\dot{p} = 4E_t - \dot{Q} \tag{20}$$

$$\dot{E}_t = P_t - E_t/\tau \tag{21}$$

For a microgrid in Figure 10 with one a single RL filter these state variables are are defined as

$$E = Li^2/2 \tag{22}$$

$$p = Li\dot{i} \tag{23}$$

$$E_t = L\dot{i}^2/2 \tag{24}$$

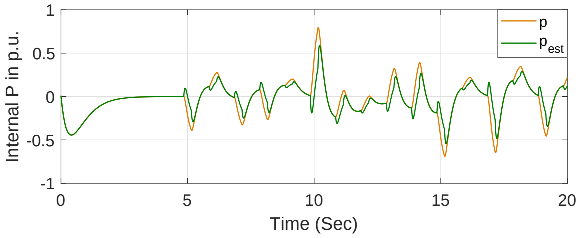

Fig. 11: Microgrid under Attack without Corrective Control

These state variables are functions of themselves and $P_t = \frac{dv}{dt}\frac{di}{dt}$ and $\dot{Q} = \frac{dv}{dt}i - \frac{di}{dt}v$ representing interactions with the rest of the system [28], [29]. This modeling approach confines the system model to a third order model which remains same in its fundamental structure independent from the actual internal system complexity.

$$x = [E \quad p \quad E_t]^T \tag{25}$$

and the energy control [30]

$$u = [\dot{Q} \quad P_t]^T \tag{26}$$

With this mapping of physical state to energy model states, we can apply the proposed switch-role corrective control (11) to the microgrid.

B. *Simulation Results: Application to a Microgrid*

The microgrid system shown in Figure 10 takes on the form given in Equation (25) where A, B, K, L, and L_p, where L is used for the observer subsystem, and L_p for the plant subsystem.

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & -2 \end{bmatrix}, \quad L = \begin{bmatrix} 10 & 1 & 0 \\ 0 & 20 & 4 \\ 0 & 0 & 28 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 \\ -1 & 0 \\ 0 & 1 \end{bmatrix}, \quad L_p = \begin{bmatrix} 40 & 1 & 0 \\ 0 & 80 & 4 \\ 0 & 0 & 118 \end{bmatrix}$$

$$C = I, \quad K = \begin{bmatrix} 6 & 5 & 4 \\ 0 & 0 & 1 \end{bmatrix}$$

In the first experiment, we simulate an attack on the system. The disturbance is random noise for a duration of 0.05 seconds, every second for a 20 second simulation. An observer is used to track the primary system and observer control is used in the primary system- in this case the observer is tracking tampered system variables. The observer values are tampered (green curve in Fig. 11), so when observer control is used in the primary system, the system does not stabilize as well under attack (orange curve in Fig. 11).

In the second experiment, we simulate the same attack on the system. This time, our observer rejects the attack signal and serves as the ground-truth (green curve in Fig. 12), and then the observer control is used in the primary system to re-stabilize and bring closer to the untampered variable values (orange curve in Fig. 12). The system returns to untampered values much faster than in the previous case because the observer is holding the ground-truth, not tampered variables.

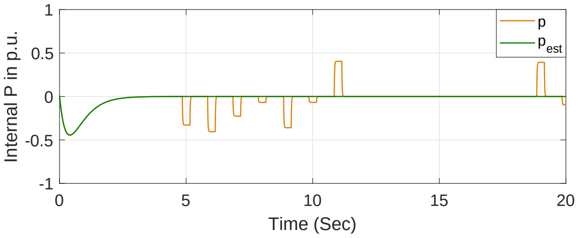

Fig. 12: Microgrid under Attack with Switch-Role Corrective Control

VI. Conclusion

This paper proposes cyber-secure observer-based corrective control under sensor deception attacks when secure state estimation is not available. Solutions are proposed for both open-loop stable and open-loop unstable LTI systems. The principal idea is to use the observer as the ground-truth, preserve its intactness, and make the plant dynamics follow the observer behavior during the attack. We showed stability of the proposed methods in the appropriate senses, and characterized the effects of the discrepancy between the observer and the plant. Numerical simulations, with an application to making cyber-secure microgrids, are shown.

The proposed corrective control strategy is a stand-alone technique which has low complexity, is easy to implement at low cost, and requires no centralized coordination. Future research directions include distributed observers and defense against a broader range of attacks.

Acknowledgement

Partial funding by the NSF EAGER project ECCS-2002570 entitled EAGER: Fundamentals of Modeling and Control for the Evolving Electric Power System Architectures, the DOE SETO project entitled Secure Monitoring and Control of Solar PV Systems through Watermarking, and by the NSF CNS-1735463 is greatly appreciated.

References

[1] D. Ding, Z. Wang, Q.-L. Han, and G. Wei, "Security control for discrete-time stochastic nonlinear systems subject to deception attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 5, pp. 779–789, 2016.

[2] M. M. Hossain and C. Peng, "Observer-based event triggering H_∞ LFC for multi-area power systems under dos attacks," *Information Sciences*, vol. 543, pp. 437–453, 2021.

[3] Y. Zhang, L. Ma, G. Wang, C. Yang, L. Zhou, and W. Dai, "Observer-based control for the two-time-scale cyber-physical systems: the dual-scale dos attacks case," *IEEE Transactions on Network Science and Engineering*, 2021.

[4] D. Wang, Z. Wang, B. Shen, and F. E. Alsaadi, "Security-guaranteed filtering for discrete-time stochastic delayed systems with randomly occurring sensor saturations and deception attacks," *International Journal of Robust and Nonlinear Control*, vol. 27, no. 7, pp. 1194–1208, 2017.

[5] F. Pasqualetti, F. Dörfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE transactions on automatic control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[6] K. G. Vamvoudakis, J. P. Hespanha, B. Sinopoli, and Y. Mo, "Detection in adversarial environments," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3209–3223, 2014.

[7] B. Satchidanandan and P. R. Kumar, "Dynamic watermarking: Active defense of networked cyber–physical systems," *Proceedings of the IEEE*, vol. 105, no. 2, pp. 219–240, 2016.

[8] D. Ding, Z. Wang, D. W. Ho, and G. Wei, "Distributed recursive filtering for stochastic systems under uniform quantizations and deception attacks through sensor networks," *Automatica*, vol. 78, pp. 231–240, 2017.

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

[10] S. Mishra, N. Karamchandani, P. Tabuada, and S. Diggavi, "Secure state estimation and control using multiple (insecure) observers," in *53rd IEEE Conference on Decision and Control*. IEEE, 2014, pp. 1620–1625.

[11] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transactions on Automatic control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[12] A.-Y. Lu and G.-H. Yang, "Secure luenberger-like observers for cyber–physical systems under sparse actuator and sensor attacks," *Automatica*, vol. 98, pp. 124–129, 2018.

[13] ——, "Secure switched observers for cyber-physical systems under sparse sensor attacks: A set cover approach," *IEEE Transactions on Automatic Control*, vol. 64, no. 9, pp. 3949–3955, 2019.

[14] Y. Zhou, K. G. Vamvoudakis, W. M. Haddad, and Z.-P. Jiang, "A secure control learning framework for cyber-physical systems under sensor attacks," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 4280–4285.

[15] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Transactions on Automatic Control*, vol. 56, no. 7, pp. 1495–1508, 2010.

[16] A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1813–1820, 2017.

[17] Y. Zhu and W. X. Zheng, "Observer-based control for cyber-physical systems with periodic dos attacks via a cyclic switching strategy," *IEEE Transactions on Automatic Control*, vol. 65, no. 8, pp. 3714–3721, 2019.

[18] D. Zhao, Z. Wang, D. W. Ho, and G. Wei, "Observer-based pid security control for discrete time-delay systems under cyber-attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 2019.

[19] J. Qi, A. F. Taha, and J. Wang, "Comparing kalman filters and observers for power system dynamic state estimation with model uncertainty and malicious cyber attacks," *IEEE Access*, vol. 6, pp. 77 155–77 168, 2018.

[20] M. S. Chong, M. Wakaiki, and J. P. Hespanha, "Observability of linear systems under adversarial attacks," in *2015 American Control Conference (ACC)*. IEEE, 2015, pp. 2439–2444.

[21] Y. Shoukry and P. Tabuada, "Event-triggered state observers for sparse sensor noise/attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 8, pp. 2079–2091, 2015.

[22] T. Huang, B. Satchidanandan, P. Kumar, and L. Xie, "An online detection framework for cyber attacks on automatic generation control," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6816–6827, 2018.

[23] T. Huang, B. Wang, J. Ramos-Ruiz, P. Enjeti, P. Kumar, and L. Xie, "Detection of cyber attacks in renewable-rich microgrids using dynamic watermarking," in *2020 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2020, pp. 1–5.

[24] E. D. Sontag, *Mathematical control theory: deterministic finite dimensional systems*. Springer Science & Business Media, 2013, vol. 6.

[25] H. V. Henderson and S. R. Searle, "On deriving the inverse of a sum of matrices," *Siam Review*, vol. 23, no. 1, pp. 53–60, 1981.

[26] N. Pogaku, M. Prodanovic, and T. C. Green, "Modeling, analysis and testing of autonomous operation of an inverter-based microgrid," *IEEE Transactions on Power Electronics*, vol. 22, no. 2, pp. 613–625, 2007.

[27] R. Brockett and J. Wood, "Application of system theory to power processing problems." vol. NASA CR-134708, 1974.

[28] M. Ilić and R. Jaddivada, "Multi-layered interactive energy space modeling for near-optimal electrification of terrestrial, shipboard and aircraft systems," *Annual Reviews in Control*, vol. 45, pp. 52–75, 2018.

[29] J. Wyatt and M. Ilic, "Time-domain reactive power concepts for nonlinear, nonsinusoidal or nonperiodic networks," in *IEEE international symposium on circuits and systems*. IEEE, 1990, pp. 387–390.

[30] R. Jaddivada and M. Ilić, "A feasible and stable distributed interactive control design in energy state space," 2021.