A Model-free False Data Injection Attack Strategy in Networked Control Systems

Xiaoyu Luo[†], Chongrong Fang[†], Chengcheng Zhao[‡], and Jianping He[†]

Abstract— **The data-driven attack strategies recently have received much attention when the full knowledge of the system model is unknown or difficult to be obtained for the adversary. Note that despite the critical parameters of the system model being unavailable for the adversary, the existing data-driven attack methods still depend on the linearity of the unknown system model. In this paper, we design a completely model-free attack strategy where the adversary with limited capability aims to compromise state variables such that the output value follows the expected trajectory. Specifically, we first construct a zeroth-order feedback optimization framework and uninterruptedly use probing signals for real-time measurements. Then, we iteratively update the attack signals along the composite direction of the gradient estimates of the objective function evaluations and the projected gradients. These objective function evaluations can be obtained only by real-time measurements. Furthermore, we characterize the optimality of these solutions via the optimality gap, which is affected by the dimensions of the attack signal, the iterations of solutions, and the convergence rate of the system. Extensive simulations are conducted to show the effectiveness of the proposed attack strategy.**

I. INTRODUCTION

Networked control systems (NCSs) are extensively applied in many practical systems, such as mobile robots, smart grids, unmanned aerial vehicles, and remote diagnostics, which are spatially distributed systems where communication networks build bridges for information transmission among physical components [1]–[3]. Recently, security issues have been becoming increasingly prominent in NCSs since communication networks as well as physical components are vulnerable to cyber attacks, which include Denial-of-Service (DoS) attacks [4] and false data injection (FDI) attacks [5]. Especially, the adversary who launches well-crafted FDI attacks can cause serious damage to NCSs while keeping stealthy. Hence, to defend against such kinds of intelligent attacks, studying the influence of potential FDI attack strategies on NCSs is beneficial to analyze the system vulnerabilities and design countermeasures to improve system security.

Lots of literature has been devoted to designing the model-based FDI attack strategy [6]–[11]. For instance, when the adversary knows information about the system model and other critical information, such as statistical properties of noise and the controller feedback matrix, Chen *et al.* [6] formulated a linear quadratic cost function to obtain the optimal attack sequences over the finite time interval, where the adversary aims to move the system state to a target state subject to the detection-avoidance constraint. With the prior information on the system model, Guo *et al.* [7] proposed an innovation-based linear attack strategy and formulated a two-stage optimization problem to obtain the worse-case attack policy. Wang constructed an optimal attack strategy to deteriorate the performance of fault detectors by solving coupled backward recursive Riccati difference equations (RDEs) [8]. In [9], the FDI attack strategy against remote state estimation with sensor-to-estimator communication rate constraint was designed. Note that the design of the above FDI attack strategies is mostly based on the full knowledge of the exact system model. However, when the system model changes dynamically with a complex environment or the exact prior information on the system model is difficult to be acquired for the adversary, the model-based attack strategies could be infeasible.

Therefore, there are lots of researchers aiming at designing data-driven FDI attack strategies [12]–[15]. Kim *et al.* [13] extended the work in [5] and presented two data-driven attack strategies based on subspace methods without the knowledge of the system parameter matrix. An *et al.* [14] formulated the attack goal as a data-based $\mathcal{L}_2$-gain composite optimization problem and proposed a new multiobjective adaptive dynamic programming (ADP) method for launching the attack policy. Zhao *et al.* [15] proposed an undetected FDI attack strategy based on the subspace identification technique to maximize the state estimation error with the constraint of undetectability and energy limitation. Note that the above attack strategies mostly require offline observations of linear systems in the finite time interval, exploit these observations to regress the parameter matrices of the linear system model. However, when the system has complicated nonlinearity, it is hard for the adversary to regress the critical system matrix parameters. Moreover, the linearity of the system model is still a crucial and implicit prior condition for these data-driven attack strategies.

Motivated by the above observations, we focus on designing a completely model-free attack strategy without any prior information about the system model and dependence on linear models. The adversary with limited capacity desires to steer the output value to a defined trajectory where

[†]: The Department of Automation, Shanghai Jiao Tong University, Key Laboratory of System Control and Information Processing, Ministry of Education of China, and Shanghai Engineering Research Center of Intelligent Control and Management, Shanghai 200240, China. E-mails: {xyl.sjtu, crfang, jphe}@sjtu.edu.cn.

[‡]: The State Key Laboratory of Industrial Control Technology and Institute of Cyberspace Research, Zhejiang University, China. E-mail: zccsq90@gmail.com.

only real-time measurements can be obtained. The main contributions are summarized as follows.

- We construct a feedback optimization framework for the design of the attack strategy, where the adversary with limited capacity has no prior information on the system model.
- We propose a model-free attack strategy that drives the output value to the expected output trajectory based on the objective function evaluations for directly updating the attack signal instead of learning the parameters of the system model. Moreover, the attack signals are constrained within the feasible solutions of the projected gradient descent method.
- We theoretically characterize the optimality of solutions via the optimality gap and analyze the impact on the optimality of the dimensions of the attack signal, the iterations of solutions, and the convergence rate of the dynamical system.

The rest of the paper is organized as follows. Section II introduces the system model and the adversary model, and formulates the FDI attack design problem. In Section III, the model-free attack strategy is designed and the optimality gap is analyzed. Simulation results are presented in Section IV. Finally, we conclude our work in Section V.

II. PROBLEM FORMULATION

A. System Dynamic Model & Adversary Model

Consider a discrete-time dynamical system

$$\begin{aligned} x_{k+1} =& f(x_k, u_k), \\ y_k =& g(x_k), \end{aligned} \tag{1}$$

where $x_k \in \mathbb{R}^n$ is the system state at time k, $u_k \in \mathbb{R}^m$ is the system input, $y_k \in \mathbb{R}^q$ is the system output.

Assumption 1: The system (1) is stable under the control of system input $u_k, \forall k \in \mathbb{N}$.

Consider the adversary can compromise the stable system and manipulate its states x_k arbitrarily and aims to steer the output value y_k^a to its expected trajectory. The dynamical system under attacks can be rewritten as

$$\begin{aligned} x_{k+1}^a =& f(x_k^a, u_k) + \Gamma\theta_k, \\ y_k^a =& g(x_k^a), \end{aligned} \tag{2}$$

where the attack selection matrix $\Gamma \in \mathbb{R}^{n\times p}$ is defined as the non-zero columns of $\mathrm{diag}(\gamma_1, \ldots, \gamma_n)$ with the binary variable $\gamma_i = 1$ if the i-th dimensional state is compromised, and $\theta_k \in \mathbb{R}^p$ is the injected false data. Then, we make the following assumption about the ability of the adversary.

Assumption 2: The capacity of the adversary is limited, i.e., $\theta_k^{\mathrm{T}}\theta_k \le R$, where R is the upper bound of attack energy.

Assumption 2 is common for the energy-constrained adversaries [16]. With Assumption 1 and 2, it is easy to obtain the following lemma to show that the compromised system (6) is still stable and controllable with the bounded FDI attacks.

Lemma 1: For the compromised system (6), there exists a unique steady-state map $x_{ss}^a : \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}^n$ such that $\forall\theta, f'(x_{ss}^a(u,\theta), u, \theta) \triangleq f(x_{ss}^a(u,\theta), u) + \Gamma\theta = x_{ss}^a(u,\theta)$. The map $x_{ss}^a(u,\theta)$ is M_x-Lipschitz with respect to θ, and the function $g(x^a)$ is M_g-Lipschitz with respect to x^a.

Remark 1: Lemma 1 is similar to [17] for guaranteeing the stability of the system. If the system under the bounded FDI attacks has no unique steady-state map x_{ss}^a, it is obvious that the system will diverse and even the original system (1) is unstable. The properties of the map $x_{ss}^a(u,\theta)$ can be ensured by the implicit function theorem [18, Theorem 1B.1]. According to Lemma 1, in the steady state we have

$$y^a = g(x_{ss}^a(u,\theta)) \triangleq h(u,\theta). \tag{3}$$

Additionally, the Lyapunov theorem in [19, Theorem 2.7], guarantees that there exists a Lyapunov function $V : \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p \to \mathbb{R}$ and parameters $\alpha_1, \alpha_2, \alpha_3 > 0$ such that

$$\alpha_1\|x^a - x_{ss}^a(u,\theta)\|^2 \le V(x^a, u, \theta) \le \alpha_2\|x^a - x_{ss}^a(u,\theta)\|^2, \tag{4}$$

$$V(f'(x_{ss}^a(u,\theta), u, \theta)) - V(x^a, u, \theta) \le -\alpha_3\|x^a - x_{ss}^a(u,\theta)\|^2, \tag{5}$$

Based on (4) and (5), the rate of the change in one step of the function value $V(x^a, u, \theta)$ as

$$\mu \triangleq \frac{2\alpha_2}{\alpha_1}(1 - \frac{\alpha_3}{\alpha_2}). \tag{6}$$

Assumption 3: The convergence rate μ satisfies $\mu < 1$.

The smaller μ is, the faster the system converges to the steady-state [20]. The formal interpretation of μ will be presented later in Lemma 4.

B. Problem Formulation

Since the prior condition that the system is linear is hard to obtain, it will be difficult to regress the critical system parameter matrix for the data-driven attack strategies. In contrast, in this paper, we aim to design a completely model-free attack strategy, which is independent of the characteristics and parameters of the system model itself.

In this work, we consider that the adversary's objective is to steer the output value y_k^a to follow its expected trajectory $\bar{y}_k$ as closely as possible. We also consider that the adversary has limited energy. Therefore, the total goal of adversaries is to reduce both the error between the true system output and expected trajectory and the consumed attack energy as much as possible. In addition, since our proposed attack strategy performs the optimization with the same objective function at each time k, we omit the subscript k and formally formulate the problem as

$$\begin{aligned} \mathcal{P}_1: \quad & \min_\theta \ \Phi(\theta, y^a) = \|y^a - \bar{y}\| + \theta^{\mathrm{T}} Q\theta \\ & \text{s.t. } y^a = h(u,\theta), \\ & \quad \theta^{\mathrm{T}}\theta \le R, \end{aligned} \tag{7}$$

where $y^a = h(u,\theta)$ is the steady-state map under attacks in (6) to guarantee the stability of the compromised system (6), $\bar{y}$ is the expected trajectory and $Q \in \mathbb{R}^{p\times p}$ is the positive definite weight matrix chosen by the adversary according

to the tradeoff between the limited attack capability and tracking deviation $\|y^a - \bar{y}\|$. We also propose a common assumption for the optimized objective function as follows.

Assumption 4: The function $\Phi(\theta, y^a)$ is M-Lipschitz with respect to θ, M_y-Lipschitz with respect to y^a, and $\inf_{\theta, y^a} \Phi(\theta, y^a) > -\infty$.

The challenges of solving problem $\mathcal{P}_1$ come from two aspects. One is the nonlinearity of the system model. For the unknown nonlinear system model (6), it is hard to regress its critical system parameters. The other is how to use the compromised measurements to guide the output value to move along the desired trajectory while reducing the consumed attack energy as much as possible. Since $h(u, \theta)$ is unknown, it is difficult to directly obtain the gradients of the objective function with respect to the independent variable θ to solve problem $\mathcal{P}_1$.

The key idea of the zeroth-order optimization is to utilize the objective function evaluations to construct gradient estimates, thus avoiding using the gradients directly. Motivated by the idea of a zeroth-order optimization framework, we aim to construct the gradient estimates of the objective function to solve problem $\mathcal{P}_1$. Different from the traditional zeroth-order optimization framework for the design of the controller with non-manipulated measurements, our design focuses on utilizing the compromised measurements to design the attack signal in the original control systems with designed controllers. Herein, we only explore the model-free attack strategy without detectors and the attack design under detector constraints will be left as future work.

III. Model-free Attack Strategy Design

In this section, we first introduce the zeroth-order optimization framework, which is the basis of our attack strategy design. Then, we utilize the real-time output values to design the attack signal. Finally, we analyze the optimality of the proposed attack strategy.

A. Preliminaries of Zeroth-order Optimization

The attack strategy design in this paper is inspired by the gradient estimates based on the residual feedback in [21].

For an objective function $\Phi(w) : \mathbb{R}^p \to \mathbb{R}$, the gradient estimate proposed in [21] is

$$\hat{\nabla}\Phi(w_k) = \frac{v_k}{\delta}(\Phi(w_k + \delta v_k) - \Phi(w_{k-1} + \delta v_{k-1})), \quad (8)$$

where v_k and v_{k-1} are independent random vectors selected uniformly from the unit sphere $\mathcal{S}_p \triangleq \{v_k \in \mathbb{R}^p : \|v_k\| = 1\}$, i.e., $v_k \sim U(\mathcal{S}_p)$ and $\delta > 0$ is the smoothing parameter. Note that only a new objective function evaluation needs to be computed each time in (8), because the objective value evaluated at the previous time $k-1$ is reused at the current time k.

According to [21, Lemma 5], $\hat{\nabla}\Phi(w_k)$ in (8) is unbiased estimate of the gradient of the Gaussian smooth approximation $\Phi_\delta(w)$ for $\Phi(w)$ at w_k, where

$$\Phi_\delta(w) = \mathbb{E}_{v \sim U(\mathcal{S}_p)}[\Phi(w + \delta v)]. \quad (9)$$

The properties of $\Phi_\delta(w)$ are shown as follows.

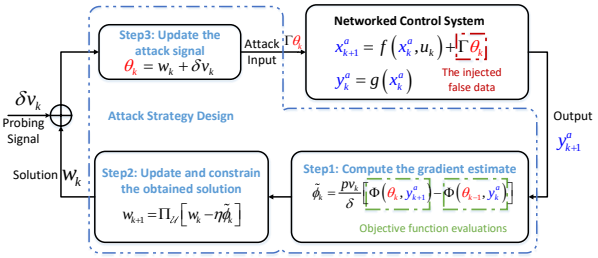


Fig. 1. The schematic of model-free attack strategy design

Lemma 2 ([17]): If $\Phi_\delta(w) : \mathbb{R}^p \to \mathbb{R}$ is $M-$Lipschitz, then for any $w \in \mathbb{R}^p, \delta > 0$ and $\Phi_\delta(w)$ defined in (9),

$$\mathbb{E}_{v \sim U(\mathbb{S}_p)}[\frac{p}{\delta}\Phi(w + \delta v)v] = \nabla\Phi_\delta(w), \quad (10a)$$

$$|\Phi_\delta(w) - \Phi(w)| \leq M\delta, \quad (10b)$$

$$\|\nabla\Phi_\delta(w) - \nabla\Phi(w)\| \leq \frac{Mp}{\delta}. \quad (10c)$$

From (10c), we know $\Phi_\delta(w)$ is $\frac{Mp}{\delta}$-smooth, i.e., its gradient $\nabla\Phi_\delta(w)$ is $\frac{Mp}{\delta}$-Lipschitz continuous.

B. Attack Strategy Design

The proposed attack strategy iteratively updates attack inputs along the composite direction of the negative gradient estimates of the objective function and the projected gradients. Such a design only utilizes the real-time measurements (i.e., the system output values) and thus makes the attack strategy intrinsically model-free.

We denote $\mathcal{U}$ as the constraint set for the limited capability of the adversary in problem $\mathcal{P}_1$. With the zeroth-order optimization framework, the proposed model-free attack strategy can be divided into three steps and the schematic of the attack strategy design is shown in Fig.1.

Step 1: Compute the gradient estimate $\tilde{\phi}_k$

$$\tilde{\phi}_k = \frac{pv_k}{\delta}[\Phi(\theta_k, y^a_{k+1}) - \Phi(\theta_{k-1}, y^a_k)], \quad (11)$$

where v_k and v_{k-1} are independent probing signals and follow the uniform distribution from the Euclidean unit sphere $\mathcal{S}_p$, i.e., $v_k \sim U(\mathcal{S}_p)$. Since only the real-time measurements are available for the adversary and it is hard to directly compute the gradients of the objective function in problem $\mathcal{P}_1$, we first utilize the probing signal v_k for measurements, which can be used to construct the objective function evaluations $\Phi(\theta_k, y^a_{k+1})$ and $\Phi(\theta_{k-1}, y^a_k)$ at the current and previous time. Herein, the historic function evaluation $\Phi(\theta_{k-1}, y^a_k)$ is reused at time $k+1$. Then we compute the gradient estimates $\tilde{\phi}_k$ of the objective function by these evaluations with (11).

Step 2: Update and constrain the obtained solution w_{k+1}

$$w_{k+1} = \Pi_{\mathcal{U}}[w_k - \eta\tilde{\phi}_k], \quad (12)$$

where $\Pi_{\mathcal{U}}[\cdot]$ is the projection onto the constrained set $\mathcal{U}$, i.e., $\Pi_{\mathcal{U}}[l_1] \equiv \arg\min_{l_2 \in \mathcal{U}} \|l_1 - l_2\|$, and step-size $0 < \eta < 1$. To constrain the obtained solutions in the feasible region set by $\mathcal{U}$, we turn to the projected gradient descent method for updating the solution w_{k+1} at time $k+1$ and solving the

optimization problem $\mathcal{P}_1$ with constraints.

Step 3: Update the attack signal θ_{k+1}

$$\theta_{k+1} = w_{k+1} + \delta v_{k+1}. \tag{13}$$

Finally, the attack signal θ_{k+1} can be obtained by perturbing the solution w_{k+1} with the probing signals δv_{k+1}.

C. Performance Analysis

Let $\Phi(\theta_k) \triangleq \Phi(\theta_k, h(u_k, \theta_k))$. We use the optimality gap, i.e.,

$$\frac{1}{T}\sum_{k=1}^{T} \mathbb{E}_{v_{[T]}}[\Phi(\theta_k) - \Phi(\theta_k^*)] \tag{14}$$

to measure the optimality of the proposed attack strategy at θ_k where θ_k^* is the optimal solution at time k and $\mathbb{E}_{v_{[k]}}$ is the expectation of $v_{[k]}$ with $v_{[k]} \triangleq (v_0, \ldots, v_k)$.

Before we characterize (14), we provide the upper bound of $\|w_{k+1} - w_{k+1}^*\|^2$ and $\|w_{k+1} - w_k\|^2$, and some supporting lemmas for auxiliary analysis. We have

$$\begin{aligned}\|w_{k+1} - w_{k+1}^*\|^2 =& \|\Pi_{\mathcal{U}}[w_k - \eta\tilde{\phi}_k] - w_{k+1}^*\|^2 \\ \overset{(s.1)}{\leq}& \|w_k - \eta\tilde{\phi}_k - w_{k+1}^*\|^2 \\ \overset{(s.2)}{\leq}& 2\|w_k - w_{k+1}^*\|^2 + 2\eta^2\|\tilde{\phi}_k\|^2, \end{aligned} \tag{15}$$

where $(s.1)$ follows from the projection property [22, Lemma 2.4] and [23], i.e., for any $l_1 \in \mathbb{R}^p$ and all $l_2 \in \mathcal{U}$, $\|\Pi_{\mathcal{U}}[l_1] - l_2\| \leq \|l_1 - l_2\|$, and $(s.2)$ follows the fact that $\|a-b\|^2 \leq 2(\|a\|^2 + \|b\|^2)$. Similarly, we have

$$\begin{aligned}\|w_{k+1} - w_k\|^2 =& \|\Pi_{\mathcal{U}}[w_k - \eta\tilde{\phi}_k] - w_k\|^2 \\ \leq& \|w_k - \eta\tilde{\phi}_k - w_k\|^2 \\ \leq& \eta^2\|\tilde{\phi}_k\|^2. \end{aligned} \tag{16}$$

Note that we replace the steady output value $h(u_k, \theta_k)$ with the real-time output value y_{k+1}^a to enter the closed-loop zeroth-order feedback optimization framework. It is unavoidable for the system to produce the error $e_\Phi(x_k^a, \theta_k)$, which is defined as

$$e_\Phi(x_k^a, \theta_k) = \Phi(\theta_k, y_{k+1}^a) - \Phi(\theta_k, h(u_k, \theta_k)). \tag{17}$$

First, we analyze the upper bound of the error $e_\Phi(x_k^a, \theta_k)$ and the recursive inequalities of two critical variables, i.e., $\mathbb{E}_{v_{[k]}}[V(x_k^a, u_k, \theta_k)]$ and $\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2]$.

Lemma 3: If Assumptions $1-3$ hold, then

$$|e_\Phi(x_k^a, \theta_k)|^2 \leq \frac{\mu M_y^2 M_g^2}{2\alpha_2} V(x_k^a, u_k, \theta_k). \tag{18}$$

Lemma 4: If Assumptions $1-3$ hold, with (11), (12) and (13), then

$$\begin{aligned}&\mathbb{E}_{v_{[k]}}[V(x_k^a, u_k, \theta_k)] \\ &\quad\leq \mu\mathbb{E}_{v_{[k]}}[V(x_{k-1}^a, u_{k-1}, \theta_{k-1})] \\ &\quad+ 4\alpha_2\eta^2 M_x^2 \mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2] + 16\alpha_2\delta^2 M_x^2 \end{aligned} \tag{19}$$

Lemma 5: If Assumptions $1-3$ hold, with (11), (12), and (13), then

$$\begin{aligned}\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2] \leq& \frac{6\eta^2 p^2 M^2}{\delta^2}\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2] + 24p^2M^2 \\ &+ \frac{3\mu p^2 M_y^2 M_g^2}{2\alpha_2\delta^2}(\mathbb{E}_{v_{[k]}}[V(x_k^a, u_k, \theta_k)] \\ &+ \mathbb{E}_{v_{[k]}}[V(x_{k-1}^a, u_{k-1}, \theta_{k-1})]) \end{aligned} \tag{20}$$

The proof of Lemma $3-5$ follows from [17], where the differences lie in the additional independent variable θ and the compromised states. Here, the proof of Lemma 4 is shown in Appendix V-A and we omit the proof of Lemma 3 and Lemma 5 due to the limited space. Lemma 3 quantifies the close relationship between $\Phi(\theta_k, y_{k+1}^a)$ and $\Phi(\theta_k, h(u_k, \theta_k))$. Lemma 4 measures the proximity of the current state x_k^a compared with the steady state $x_{ss}^a(u_k, \theta_k)$. Lemma 5 reflects the first order smoothness of the objective function evaluation $\Phi(\theta_k, y_{k+1}^a)$ at solution w_k.

Next, we provide the following theorem to characterize the optimality of the obtained solutions.

Theorem 1: Suppose that Assumptions $1-3$ hold, for any given precision $\epsilon > 0$ such that $|\Phi_\delta(\theta) - \Phi(\theta)| \leq \epsilon$, let $\delta = \frac{\epsilon}{M}$ and $\eta = \frac{\kappa\epsilon}{pT}$ with $\kappa \in (0, \kappa^*)$, where

$$\kappa^* = \mathcal{O}\left(\min\left\{\frac{T\sqrt{\mu(1+\mu)}}{\mu}, \frac{(1-\mu)T}{\sqrt{\mu(1+\mu)}}\right\}\right),$$

then we have

$$\begin{aligned}&\frac{1}{T}\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\Phi(\theta_k) - \Phi(\theta_k^*)] \\ &\qquad= \mathcal{O}\left(\frac{p^2(1+\mu)(1+\sqrt{1+\mu})}{(1-\rho)T^2} + \frac{\mu p^2}{T}\right), \end{aligned} \tag{21}$$

where $\rho \in (0,1)$ is the maximum eigenvalue of matrix P given by (28), i.e., $P = \begin{bmatrix} p_{11} & \sqrt{p_{12}p_{21}} \\ \sqrt{p_{12}p_{21}} & p_{22} \end{bmatrix}$ with

$$\begin{aligned} p_{11} =& \frac{6p^2\eta^2}{\delta^2}(M^2 + \mu M_x^2 M_y^2 M_g^2), \\ p_{12} =& \frac{3\mu p^2 M_y^2 M_g^2}{2\alpha_2\delta^2}(1+\mu), \\ p_{21} =& 4\alpha_2\eta^2 M_x^2, \\ p_{22} =& \mu, \\ d_1 =& 24p^2(M^2 + \mu M_x^2 M_y^2 M_g^2), \\ d_2 =& 16\alpha_2\delta^2 M_x^2. \end{aligned} \tag{22}$$

Moreover,

$$\rho = \mathcal{O}\left(\max\left\{\frac{(1-\mu)^2}{1+\mu}, \mu\right\} + 1 - \mu\right).$$

Proof: Please see Appendix V-B. ∎

Theorem 1 shows the optimality gap is related to the dimensions p of the attack signal, the convergence rate μ of the system, and the iterations T. As the iterations T increase gradually, the optimality gap decreases and it can even decay to zero as long as T is large enough.

IV. Simulation Results

In this section, we evaluate the performance of the proposed attack strategy, i.e., we analyze the tracking performance and the optimality of solutions.

Consider the following system

$$\begin{aligned} x_{k+1} =& Ax_k + Bu_k, \\ y_k =& Cx_k, \end{aligned} \tag{23}$$

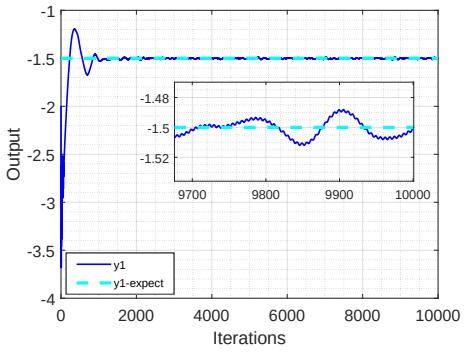
where $u_k = -Kx_k$ with $K = [1.5 \ \ -1.5; 0.2 \ \ 0.1], A = [0 \ \ 1; 2 \ \ -1], B = [0 \ \ 0; 1 \ \ 0], C = [1 \ \ 1]$. It is stable, controllable, and observable. We set the initial state $x_1 = [1; -3]$, the probing signal $v_k = [\cos(k); \sin(k)]/\sqrt{2}$ to satisfy $\|v_k\| = 1$, the initial solution w_1 is random and follows the standard uniform distribution. The smoothing parameter $\delta = 10^{-3}$, the step-size $\eta = 7.5 \times 10^{-5}$, the attack selection matrix $\Gamma = I_2$ and the weight matrix $Q = 3I_2$ where I_2 is the two-dimensional diagonal unit matrix. We define two types of the expected output trajectories, including the static trajectory $\bar{y}_1 = -1.5$ and dynamic output trajectory $\bar{y}_2 = 10^{-4}k$ with respect to time k. Each data point in the following figures represents an ensemble average of 50 trials.

First, we analyze the tracking performance with different desired output trajectories. As shown in Fig. 2, the output value of the system under the proposed attack strategy has the ability of tracking the expected output trajectory whether the trajectory is static or dynamic. Especially, Fig. 2(a) and Fig. 2(b) illustrate that the output values fluctuate along the desired trajectory. Note that the phenomenon of fluctuation is normal since the output values are constantly perturbed by the time-varying probing signal v_k.

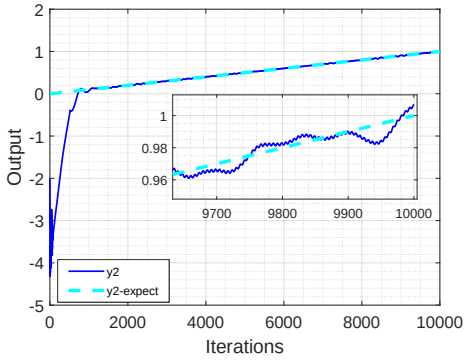
Then, we illustrate the optimality of solutions via the optimality gap $\Phi(\theta_k) - \Phi(\theta^*)$, which is shown in Fig. 3. When the expected trajectory is static, i.e., $\bar{y}_1 = -1.5$, we find that the obtained solution is close to the optimal solution and the optimality gap converges to about 0.02, shown in Fig. 3(a). When the expected trajectory is time-varying, i.e., $\bar{y}_2 = 10^{-4}k$, in Fig. 3(b), the obtained solutions also approach the optimal one and the upper bound of the optimality gap does not exceed 0.11. To sum up, the proposed model-free attack strategy can obtain the suboptimal attack signals that drive the output values to the desired output trajectory by only utilizing the real-time compromised measurements.

V. Conclusion

We considered the problem of designing a model-free attack strategy where the adversary with limited capacity aims to make the output value follow the desired trajectory without any prior system model information. The designed attack strategy is model-free since only real-time measurements are required. These measurements are used to compute objective function evaluations and gradient estimates are constructed to update the attack signal based on these objective function evaluations at the previous and current time. Moreover,



(a)



(b)

Fig. 2. Tracking performance under different expected output trajectories. (a) Static trajectory $\bar{y}_1 = -1.5$ (b) Dynamic trajectory $\bar{y}_2 = 10^{-4}k$

considering the adversary has limited capability, we constrained the obtained solutions within the feasible region by the projected gradient descent method. Finally, we analyzed the optimality of solutions and established its dependence on the dimensions of the attack signal, the iterations, and the convergence rate of the system. Future works include the design of attack strategies with partial observations and detector constraints.

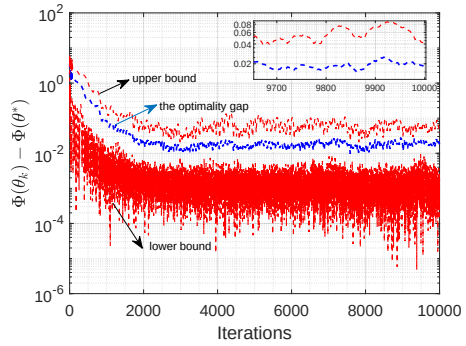
Appendix

A. Proof of Lemma 4

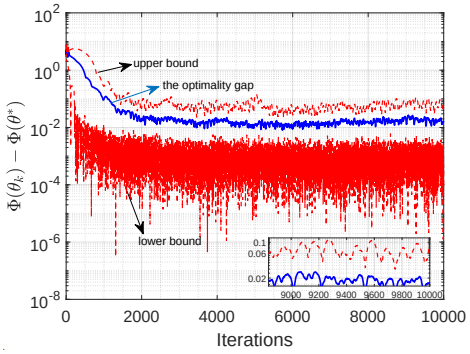
Based on (4), we have

$$\begin{aligned} &V(x_k^a, u_k, \theta_k) \le \alpha_2 \|x_k^a - x_{ss}^a(u_k, \theta_k)\|^2 \\ &= \alpha_2 \|x_k^a - x_{ss}^a(u_{k-1}, \theta_{k-1}) \\ &+ x_{ss}^a(u_{k-1}, \theta_{k-1}) - x_{ss}^a(u_k, \theta_k)\|^2 \\ &\overset{(s.1)}{\le} 2\alpha_2 (\|x_k^a - x_{ss}^a(u_{k-1}, \theta_{k-1})\|^2 \\ &+ \|x_{ss}^a(u_{k-1}, \theta_{k-1}) - x_{ss}^a(u_k, \theta_k)\|^2) \\ &\overset{(s.2)}{\le} \mu V(x_{k-1}^a, u_{k-1}, \theta_{k-1}) + 2\alpha_2 M_x^2 \|\theta_k - \theta_{k-1}\|^2, \end{aligned}$$

where $(s.1)$ follows the fact that $\|a+b\|^2 \le 2(\|a\|^2 + \|b\|^2)$ and $(s.2)$ follows from (4), (5), (6), and the Lipschitz continuity of $x_{ss}^a(u_k, \theta_k)$. The upper bound of $\mathbb{E}_{v_{[k]}}[\|\theta_k -$



(a)



(b)

Fig. 3. The optimality gap under different expected output trajectories. (a) Static trajectory $\bar{y}_1 = -1.5$ (b) Dynamic trajectory $\bar{y}_2 = 10^{-4}k$

$\theta_{k-1}\|^2]$ is given as

$$\begin{aligned}
&\mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_{k-1}\|^2] \\
&\quad = \mathbb{E}_{v_{[k]}}[\|w_k - w_{k-1} + \delta v_k - \delta v_{k-1}\|^2] \\
&\quad \overset{(s.1)}{\leq} \mathbb{E}_{v_{[k]}}[2\|w_k - w_{k-1}\|^2 + 2\delta^2\|v_k - v_{k-1}\|^2] \\
&\quad \overset{(s.2)}{\leq} 2\eta^2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2] + 2\delta^2\mathbb{E}_{v_{[k]}}[2\|v_k\|^2 + 2\|v_{k-1}\|^2] \\
&\quad \overset{(s.3)}{\leq} 2\eta^2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2] + 8\delta^2,
\end{aligned}$$

where $(s.1)$ follows that $\mathbb{E}[(a+b)^2] \leq 2\mathbb{E}[a^2 + b^2]$, $(s.2)$ follows from (16) and $\|a-b\|^2 \leq 2(\|a\|^2 + \|b\|^2)$, and $(s.3)$ follows the fact that $\|v_k\| = 1$ since v_k is selected uniformly at random from the unit sphere.

Combining the above results, we can infer that (19) holds.

B. Proof of Theorem 1

Since the objective function $\Phi(\theta_k)$ is convex, the Gaussian smooth approximation of $\Phi(\theta_k)$ is also convex [24]. With (10b), then we have

$$\Phi(\theta_k) - \Phi(\theta_k^*) \leq \Phi_\delta(\theta_k) - \Phi_\delta(\theta_k^*) + 2M\delta. \tag{24}$$

With (10c), the Taylor expansion of $\Phi_\delta(\theta_k)$ at solution θ_k^* is shown as

$$\begin{aligned}
\Phi_\delta(\theta_k) \leq &\Phi_\delta(\theta_k^*) + \nabla\Phi_\delta(\theta_k^*)^{\mathrm{T}}(\theta_k - \theta_k^*) \\
&+ \frac{M^2p^2}{2\delta^2}\|\theta_k - \theta_k^*\|^2,
\end{aligned} \tag{25}$$

where θ_k^* is the optimal solution of the problem $\mathcal{P}_1$ at time k. Taking the expectation of $v_{[k]}$ at both ends of the inequality (25), then we have

$$\begin{aligned}
&\mathbb{E}_{v_{[k]}}[\Phi_\delta(\theta_k)] - \mathbb{E}_{v_{[k]}}[\Phi_\delta(\theta_k^*)] \leq \\
&\quad \mathbb{E}_{v_{[k]}}[\nabla\Phi_\delta(\theta_k^*)^{\mathrm{T}}(\theta_k - \theta_k^*)] + \frac{M^2p^2}{2\delta^2}\mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_k^*\|^2].
\end{aligned}$$

Since

$$\begin{aligned}
&\mathbb{E}_{v_{[k]}}[\nabla\Phi_\delta(\theta_k^*)^{\mathrm{T}}(\theta_k - \theta_k^*)] \leq \\
&\quad \frac{1}{2}(\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(\theta_k^*)\|^2] + \mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_k^*\|^2])
\end{aligned}$$

where the inequality follows the fact that for $\forall a_1, a_2$,

$$\mathbb{E}[a_1^{\mathrm{T}}a_2] \leq (\mathbb{E}[\|a_1\|^2]\mathbb{E}[\|a_2\|^2])^{\frac{1}{2}} \leq \frac{1}{2}(\mathbb{E}[\|a_1\|^2] + \mathbb{E}[\|a_2\|^2]),$$

then it can be inferred that

$$\begin{aligned}
\mathbb{E}_{v_{[k]}}[\Phi_\delta(\theta_k)] \leq \mathbb{E}_{v_{[k]}}[\Phi_\delta(\theta_k^*)] &+ \underbrace{\frac{1}{2}\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(\theta_k^*)\|^2]}_{①} \\
&+ \underbrace{(\frac{1}{2} + \frac{M^2p^2}{2\delta^2})\mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_k^*\|^2]}_{②}.
\end{aligned}$$

Next, we analyze the upper bound of the item ① and ②.

$$\begin{aligned}
① =&\frac{1}{2}\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k^* + \delta v_k)\|^2], \\
=&\frac{1}{2}\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k + \delta v_k) - (\nabla\Phi_\delta(w_k + \delta v_k) \\
&-\nabla\Phi_\delta(w_k^* + \delta v_k))\|^2], \\
\overset{(s.1)}{\leq}& \mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k + \delta v_k)\|^2] + \mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k + \delta v_k) \\
&-\nabla\Phi_\delta(w_k^* + \delta v_k)\|^2], \\
\overset{(s.2)}{\leq}& \mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(\theta_k)\|^2] + \frac{M^2p^2}{\delta^2}\mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_k^*\|^2], \\
=&\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k) - (\nabla\Phi_\delta(w_k) - \nabla\Phi_\delta(\theta_k))\|^2] \\
&+\frac{M^2p^2}{\delta^2}\mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_k^*\|^2], \\
\overset{(s.3)}{\leq}& 2\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k)\|^2] + 2M^2p^2\mathbb{E}_{v_{[k]}}[\|v_k\|^2] \\
&+\frac{M^2p^2}{\delta^2}\mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_k^*\|^2], \\
=&2\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k)\|^2] + 2M^2p^2 + \frac{M^2p^2}{\delta^2}\mathbb{E}_{v_{[k]}}[\|\theta_k - \theta_k^*\|^2],
\end{aligned}$$

where $(s.1)$ follows the fact that $\|b\|^2 = \|a - (a-b)\|^2 \leq 2\|a\|^2 + 2\|a-b\|^2$, $(s.2)$ follows from (10c), i.e., $\Phi_\delta(\theta_k)$ is $\frac{Mp}{\delta}-$ smoothness, and $(s.3)$ follows from (10c) and

$\|\delta v_k\|^2 = \delta^2\|v_k\|^2$.

$$
\begin{aligned}
② =&(\frac{1}{2}+\frac{M^2p^2}{2\delta^2})\mathbb{E}_{v_{[k]}}[\|w_k - w_k^*\|^2],\\
\overset{(s.1)}{\leq}&(\frac{1}{2}+\frac{M^2p^2}{2\delta^2})(2\mathbb{E}_{v_{[k]}}[\|w_{k-1} - w_k^*\|^2] + 2\eta^2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2]),\\
\overset{(s.2)}{\leq}&(\frac{1}{2}+\frac{M^2p^2}{2\delta^2})(2\mathbb{E}_{v_{[k]}}[\|w_{k-1} - w_k\|^2] + 2\eta^2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2]),\\
\overset{(s.3)}{\leq}&(\frac{1}{2}+\frac{M^2p^2}{2\delta^2})4\eta^2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2],\\
=&(\frac{2\delta^2+2M^2p^2}{\delta^2})\eta^2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2],
\end{aligned}
$$

where $(s.1)$ follows from (15), $(s.2)$ follows that $\|w_{k-1} - w_k^*\|^2 \leq \|w_{k-1} - w_k\|^2$, and $(s.3)$ follows from (16).

The second moment of the gradient of $\Phi_\delta(w_k)$ at solution w_k is $\|\nabla\Phi_\delta(w_k)\|^2$ and we have

$$
\begin{aligned}
&\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k)\|^2]\\
&= \mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k - (\tilde{\phi}_k - \nabla\Phi_\delta(w_k))\|^2],\\
&\leq 2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2] + 2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k - \nabla\Phi_\delta(w_k)\|^2],
\end{aligned}
$$

where the inequality follows the fact that $\mathbb{E}[(a-b)^2] \leq 2(\mathbb{E}[a^2] + \mathbb{E}[b^2])$. Since

$$
\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k - \nabla\Phi_\delta(w_k)\|^2] \leq \mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2],
$$

which follows from (58) in [17, Theorem 8], with (20),

$$
\begin{aligned}
\mathbb{E}_{v_{[k]}}[\|\nabla\Phi_\delta(w_k)\|^2] \leq& \frac{24\eta^2p^2M^2}{\delta^2}\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2] + 96p^2M^2\\
&+ \frac{6\mu p^2M_y^2M_g^2}{\alpha_2\delta^2}(\mathbb{E}_{v_{[k]}}[V(x_k^a, u_k, \theta_k)]\\
&+ \mathbb{E}_{v_{[k]}}[V(x_{k-1}^a, u_{k-1}, \theta_{k-1})]).
\end{aligned}
$$

Rearranging the above items, thus we have

$$
\begin{aligned}
&\mathbb{E}_{v_{[k]}}[\Phi_\delta(\theta_k)] - \mathbb{E}_{v_{[k]}}[\Phi_\delta(\theta_k^*)]\\
&\leq (2 + \frac{54M^2p^2}{\delta^2})\eta^2\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2] + 194M^2p^2\\
&+ \frac{12\mu p^2M_y^2M_g^2}{\alpha_2\delta^2}(\mathbb{E}_{v_{[k]}}[V(x_k^a, u_k, \theta_k)]\\
&+ \mathbb{E}_{v_{[k]}}[V(x_{k-1}^a, u_{k-1}, \theta_{k-1})]).
\end{aligned}
$$

Then, it follows that

$$
\begin{aligned}
&\frac{1}{T}\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\Phi_\delta(\theta_k) - \Phi_\delta(\theta_k^*)]\\
&\leq (\frac{2}{T} + \frac{54M^2p^2}{\delta^2T})\eta^2\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\|\tilde{\phi}_{k-1}\|^2] + 194M^2p^2\\
&+ \frac{12\mu p^2M_y^2M_g^2}{\alpha_2\delta^2T}\sum_{k=1}^{T}(\mathbb{E}_{v_{[T]}}[V(x_k^a, u_k, \theta_k)]\\
&+ \mathbb{E}_{v_{[T]}}[V(x_{k-1}^a, u_{k-1}, \theta_{k-1})]) \qquad (26)
\end{aligned}
$$

To guarantee $|\Phi_\delta(w) - \Phi(w)| \leq \epsilon$, we set $\delta = \frac{\epsilon}{M}$. Combined (19), (24) and (26), we obtain

$$
\begin{aligned}
&\frac{1}{T}\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\Phi(\theta_k) - \Phi(\theta_k^*)]\\
&\leq \frac{\eta^2p^2}{\delta^2T}(\frac{2\delta^2}{p^2} + 54M^2 + 48\mu M_x^2M_y^2M_g^2)\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\|\tilde{\phi}_{k-1}\|^2]\\
&+ \frac{12\mu(\mu+1)p^2M_y^2M_g^2}{\alpha_2\delta^2T}\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[V(x_{k-1}^a, u_{k-1}, \theta_{k-1})]\\
&+ \frac{192\mu p^2M_x^2M_y^2M_g^2}{T} + 194M^2p^2 + 2M\delta. \qquad (27)
\end{aligned}
$$

Since $\mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2]$ and $\mathbb{E}_{v_{[k]}}[V(x_k^a, u_k, \theta_k)]$ are coupled variables, we rely on [17, Lemma 11], which shows the upper bound of the partial sum of non-negative coupled series, to analyze (27).

Combining (19) and (20), we can obtain a compacted form, which is shown as

$$
\begin{aligned}
&\begin{bmatrix} \mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_k\|^2] \\ \mathbb{E}_{v_{[k]}}[\sqrt{\frac{p_{12}}{p_{21}}}V(x_k^a, u_k, \theta_k)] \end{bmatrix} \preceq\\
&P\begin{bmatrix} \mathbb{E}_{v_{[k]}}[\|\tilde{\phi}_{k-1}\|^2] \\ \mathbb{E}_{v_{[k]}}[\sqrt{\frac{p_{12}}{p_{21}}}V(x_{k-1}^a, u_{k-1}, \theta_{k-1})] \end{bmatrix} + \begin{bmatrix} d_1 \\ \sqrt{\frac{p_{12}}{p_{21}}}d_2 \end{bmatrix},
\end{aligned}
$$

where $P = \begin{bmatrix} p_{11} & \sqrt{p_{12}p_{21}} \\ \sqrt{p_{12}p_{21}} & p_{22} \end{bmatrix}$ with

$$
\begin{aligned}
p_{11} =& \frac{6p^2\eta^2}{\delta^2}(M^2 + \mu M_x^2M_y^2M_g^2),\\
p_{12} =& \frac{3\mu p^2M_y^2M_g^2}{2\alpha_2\delta^2}(1+\mu),\\
p_{21} =& 4\alpha_2\eta^2M_x^2,\\
p_{22} =& \mu,\\
d_1 =& 24p^2(M^2 + \mu M_x^2M_y^2M_g^2),\\
d_2 =& 16\alpha_2\delta^2M_x^2. \qquad (28)
\end{aligned}
$$

Then, we have

$$
\begin{aligned}
&\max\{\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\|\tilde{\phi}_{k-1}\|^2], \sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\sqrt{\frac{p_{12}}{p_{21}}}V(x_{k-1}^a, u_{k-1}, \theta_{k-1})]\}\\
&\leq (\rho^T + \frac{1}{1-\rho})B_1 + \frac{T}{1-\rho}(d_1 + \sqrt{\frac{p_{12}}{p_{21}}}d_2), \qquad (29)\\
&= \mathcal{O}\left(\frac{T}{1-\rho}(p^2 + \mu p^2 + \frac{p\delta}{\eta})\right) \qquad (30)
\end{aligned}
$$

where $B_1 = \mathbb{E}[\|\tilde{\phi}(w_1)\|^2] + \mathbb{E}[\sqrt{\frac{p_{12}}{p_{21}}}V(x_1^a, u_1, \theta_1)]$ and $\rho < 1$ is the maximum singular value of the matrix P.

By solving the characteristic equation $|\lambda I - P| = 0$ with eigenvalues λ, then

$$
\begin{aligned}
\rho =& \frac{p_{11}+p_{22}}{2} + \sqrt{(\frac{p_{11}-p_{22}}{2})^2 + p_{12}p_{21}}\\
\leq& \frac{p_{11}+p_{22}}{2} + |\frac{p_{11}-p_{22}}{2}| + \sqrt{p_{12}p_{21}}\\
=& \max\{p_{11}, p_{22}\} + \sqrt{p_{12}p_{21}}, \qquad (31)
\end{aligned}
$$

To guarantee $\rho < 1$, we need to set δ and η such that

$$p_{11} + \sqrt{p_{12}p_{21}} < 1, \quad p_{22} + \sqrt{p_{12}p_{21}} < 1. \tag{32}$$

Then, combined (27) and (29), it follows that

$$\frac{1}{T}\sum_{k=1}^{T}\mathbb{E}_{v_{[T]}}[\Phi(\theta_k) - \Phi(\theta_k^*)] \leq l_3 + (l_1 + \sqrt{\frac{p_{21}}{p_{12}}}l_2)\left\{(\rho^T + \frac{1}{1-\rho})B_1 + \frac{T}{1-\rho}(d_1 + \sqrt{\frac{p_{12}}{p_{21}}}d_2)\right\} \tag{33}$$

where

$$\begin{aligned} l_1 =& \frac{2\eta^2}{T} + \frac{p^2}{\delta^2 T}(54M^2\eta^2 + 48\mu M_x^2 M_y^2 M_g^2\eta^2), \\ l_2 =& \frac{12\mu(\mu+1)p^2 M_y^2 M_g^2}{\alpha_2 \delta^2 T}, \\ l_3 =& \frac{\mu p^2 M_x^2 M_y^2 M_g^2}{T} + 194M^2p^2 + 2M\delta. \end{aligned}$$

Due to $\delta = \frac{\epsilon}{M}$, we set $\eta = \frac{\kappa\epsilon}{pT}$ such that $\frac{p^4\eta^2}{\epsilon^2}$ and $\frac{p^2}{T}$ have the same order. Then, the order of (33) is shown as (21). The parameter κ is set to satisfy (32), i.e.,

$$\begin{aligned} \xi_1\kappa^2 + \xi_2\kappa < 1, \\ \xi_3 + \xi_2\kappa < 1, \end{aligned} \tag{34}$$

where

$$\begin{aligned} \xi_1 =& \frac{6M^2(M^2 + \mu M_x^2 M_y^2 M_g^2)}{T^2}, \\ \xi_2 =& \frac{MM_xM_yM_g}{T}\sqrt{6\mu(1+\mu)}, \\ \xi_3 =& \mu. \end{aligned}$$

The feasible range is denoted by $(0, \kappa^*)$. Based on (34), we have

$$\begin{aligned} \kappa^* =& \min\left\{\frac{-\xi_2 + \sqrt{\xi_2^2 + 4\xi_1}}{2\xi_1}, \frac{1-\xi_3}{\xi_2}\right\}, \\ =& \mathcal{O}\left(\min\left\{\frac{T\sqrt{\mu(1+\mu)}}{\mu}, \frac{(1-\mu)T}{\sqrt{\mu(1+\mu)}}\right\}\right), \\ \rho =& \max\left\{\xi_1\kappa^2, \xi_3\right\} + \xi_2\kappa, \\ =& \mathcal{O}\left(\max\left\{\frac{(1-\mu)^2}{1+\mu}, \mu\right\} + 1 - \mu\right). \end{aligned}$$

REFERENCES

[1] P. Antsaklis and J. Baillieul, "Special issue on technology of networked control systems," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 5–8, 2007.

[2] R. A. Gupta and M.-Y. Chow, "Networked control system: Overview and research trends," *IEEE transactions on industrial electronics*, vol. 57, no. 7, pp. 2527–2535, 2009.

[3] X.-M. Zhang, Q.-L. Han, X. Ge, D. Ding, L. Ding, D. Yue, and C. Peng, "Networked control systems: A survey of trends and techniques," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 1, pp. 1–17, 2019.

[4] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Preprints of the 1st workshop on Secure Control Systems*, 2010, pp. 1–6.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, 2011.

[6] Y. Chen, S. Kar, and J. M. Moura, "Optimal attack strategies subject to detection constraints against cyber-physical systems," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 1157–1168, 2017.

[7] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, "Worst-case stealthy innovation-based linear attack on remote state estimation," *Automatica*, vol. 89, pp. 117–124, 2018.

[8] X.-L. Wang, "Optimal attack strategy against fault detectors for linear cyber-physical systems," *Information Sciences*, vol. 581, pp. 390–402, 2021.

[9] H. Zhang, P. Cheng, J. Wu, L. Shi, and J. Chen, "Online deception attack against remote state estimation," *IFAC Proceedings Volumes*, vol. 47, no. 3, pp. 128–133, 2014.

[10] C. Fang, Y. Qi, J. Chen, R. Tan, and W. X. Zheng, "Stealthy actuator signal attacks in stochastic control systems: Performance and limitations," *IEEE Transactions on Automatic Control*, vol. 65, no. 9, pp. 3927–3934, 2019.

[11] X. Luo, C. Zhao, C. Fang, and J. He, "Submodularity-based false data injection attack scheme in multi-agent dynamical systems," *arXiv preprint arXiv:2201.06017*, 2022.

[12] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *2011 IEEE international conference on smart grid communications (SmartGridComm)*. IEEE, 2011, pp. 244–248.

[13] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1102–1114, 2014.

[14] L. An and G.-H. Yang, "Data-driven coordinated attack policy design based on adaptive $\mathcal{L}_2$-gain optimal theory," *IEEE Transactions on Automatic Control*, vol. 63, no. 6, pp. 1850–1857, 2017.

[15] Z. Zhao, Y. Huang, Z. Zhen, and Y. Li, "Data-driven false data-injection attack design and detection in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 51, no. 12, pp. 6179–6187, 2020.

[16] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal denial-of-service attack scheduling with energy constraint," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 3023–3028, 2015.

[17] Z. He, S. Bolognani, J. He, F. Dörfler, and X. Guan, "Model-free nonlinear feedback optimization," *arXiv preprint arXiv:2201.02395*, 2022.

[18] A. L. Dontchev and R. T. Rockafellar, *Implicit functions and solution mappings*. Springer, 2009, vol. 543.

[19] N. Bof, R. Carli, and L. Schenato, "Lyapunov theory for discrete time systems," *arXiv preprint arXiv:1809.05289*, 2018.

[20] G. Belgioioso, D. Liao-McPherson, M. H. de Badyn, S. Bolognani, J. Lygeros, and F. Dörfler, "Sampled-data online feedback equilibrium seeking: Stability and tracking," *arXiv preprint arXiv:2103.13988*, 2021.

[21] Y. Zhang, Y. Zhou, K. Ji, and M. M. Zavlanos, "A new one-point residual-feedback oracle for black-box learning and control," *Automatica*, vol. 136, p. 110006, 2022.

[22] P. Jain, P. Kar *et al.*, "Non-convex optimization for machine learning," *Foundations and Trends® in Machine Learning*, vol. 10, no. 3-4, pp. 142–363, 2017.

[23] A. Nedić and J. Liu, "Distributed optimization for control," *Annual Review of Control, Robotics, and Autonomous Systems*, vol. 1, pp. 77–103, 2018.

[24] S. Liu, X. Li, P.-Y. Chen, J. Haupt, and L. Amini, "Zeroth-order stochastic projected gradient descent for nonconvex optimization," in *IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2018, pp. 1179–1183.