2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

Optimal Sequential False Data Injection Attack Scheme: Finite-time Inverse Convergence

Xiaoyu Luo†, Chongrong Fang†, Chengcheng Zhao‡, Peng Cheng‡, and Jianping He†

Abstract— **In this paper, we explore the relationship between the injected attack signal and the attack selection strategy in networked control systems where the adversary desires to steer the system state to the expected malicious one. We construct a sequential attack framework, i.e., the injected false data varies with the sampling time in discrete-time systems, and then derive an optimal sequential FDI attack strategy. The optimal sequential FDI attack strategy reveals the strongly coupled relationship between the injected attack signal and the attack selection strategy. Furthermore, we prove the finite-time inverse convergence of the critical parameters in the injected optimal attack signal by discrete-time Lyapunov analysis, which enables the efficient off-line design of the attack strategy and saves computing sources. Extensive simulations are conducted to show the effectiveness of the injected optimal sequential attack and the relationship between the attack signal and the attack selection strategy.**

I. INTRODUCTION

Security issues are becoming increasingly prominent in networked control systems (NCSs) as network technologies are extensively used to connect physical components within a control loop [1]. In NCSs, false data injection (FDI) — whereby an adversary injects false data by manipulating sensor readings or communication channels — is a commonly encountered form of attack [2]. Crucially, through an FDI attack, an adversary can cause significant damage to control components while remaining undetected.

Considerable efforts have been devoted to studying the effects of potential FDI attacks [3]–[7] and designing the optimal FDI attack strategies [8]–[10]. For instance, Chen *et al.* [8] found an optimal attack strategy to balance the control objective and the detection avoidance objective. Li *et al.* derived the optimal linear attack vector injected in the sensor readings to degrade the system estimation performance [9]. Most of these works focus on the design of the injected optimal attack signal to meet the given objective function. Besides, there are some researchers aiming at developing the FDI attack selection strategy [11]–[13]. Wu *et al.* solved an optimal switching data injection attack design problem where only one actuator is compromised each time to minimize the quadratic cost function [11]. In [13], the adversary with limited capability aims to select a subset of agents and manipulate their local multi-dimensional states to maximize the consensus convergence error by utilizing the submodularity optimization theory. It shows distinct attack effects under different attack selection strategies.

Note that there exist two interesting problems worthy of further investigation. One is to explore the relationship between the injected attack signal and the attack selection strategy. It is significant to build an analytic expression for both and analyze how the attack selection strategy influences the injected attack signal. The other is to excavate the property of the injected optimal attack signal. It is intriguing and promising to demonstrate the characteristic of the injected attack signal. Meanwhile, it is advantageous to design resilient algorithms to improve the system's security.

Motivated by the above observations, in this paper, we study the relationship between the injected optimal sequential attack signal and the attack selection strategy. Meanwhile, we desire to seek the potential property of the injected attack signal where the adversary aims to steer the system state value to an expected malicious one in a discrete-time system. The main contributions are summarized as follows.

- We construct a sequential attack framework based on dynamic programming where the adversary injects false data over sampling times and expects to drive the system state to a desired malicious one.
- We derive an analytical closed-form expression between the optimal sequential attack signal and the attack selection strategy, in which they are deeply coupled. Moreover, the attack signal is also a linear function concerning the system state.
- We theoretically characterize the finite-time inverse convergence of the critical parameters in the obtained optimal sequential attack signal via the discrete-time Lyapunov analysis, which contributes to saving resources in calculating attack signals offline.

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 optimal sequential attack strategy is designed and the convergence of the critical parameters in the injected attack signal is analyzed. Simulation results are presented in Section IV. Finally, we conclude our work in Section V.

Notations. Let $\mathbb{R}$ denote the set of real numbers. For a vector $l_1 \in \mathbb{R}^p$, we let $\|l_1\|_R^2$ denote $l_1^{\mathrm{T}} R l_1$. We denote

This work was supported by the National Natural Science Foundation of China under Grant 62103266, 62273305 and 61833015.

†: 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-mails: {zccsq90@gmail.com, lunarheart@zju.edu.cn.}

I_n and 1_n as the n-dimensional diagonal unit matrix and column vector with all elements of 1, respectively. For a matrix L_1, we let L_1^* denote its Hermitian matrix.

II. PROBLEM FORMULATION

A. System Dynamic Model & Adversary Model

Consider a discrete-time dynamical system

$$x_{k+1} = A_k x_k + B_k u_k, \tag{1}$$

where $A_k \in \mathbb{R}^{n\times n}$, $B_k \in \mathbb{R}^{n\times m}$ are the system matrices, $x_k \in \mathbb{R}^n$ is the system state at time k, and $u_k \in \mathbb{R}^m$ is the system input. We set the linear feedback controller as $u_k = L_k x_k$. Then, we have $x_{k+1} = W_k x_k$ with $W_k = A_k + B_k L_k$.

Consider an adversary can compromise the stable system (1) by altering the original control law u_k or deviating the control signals from the true values, thus indirectly manipulating the system states x_k. Meanwhile, the adversary has the ability to select which agent to tamper with. The dynamic system under attacks can be rewritten as

$$x^a_{k+1} = W_k x^a_k + \Gamma_k \theta_k, \tag{2}$$

where the attack selection strategy $\Gamma_k = [\gamma_1, \dots, \gamma_n]^{\mathrm{T}} \in \mathbb{R}^n$ with the binary variable $\gamma_i = 1$ if the i-th agent is compromised, and $\theta_k \in \mathbb{R}$ is the injected attack signal. Then, we make the following assumptions about the ability of the adversary and the definition of a sequential FDI attack.

Assumption 1: The adversary knows the exact knowledge of the system model.

Assumption 1 is a common and implicit condition for the adversary to inject false data successfully [14].

Definition 1: (Sequential FDI attack) An FDI attack is called sequential if it injects false data as the sequential sampling time k.

B. Problem Formulation

In this work, we consider that the adversary's objective is to inject the false data $\Gamma_k\theta_k$ and steer the system state to the expected malicious one as closely as possible in finite time. We also consider that the adversary desires to save the attack energy. Therefore, the total goal of the adversary is to reduce both the error between the true system state and the expected malicious one and the consumed attack energy as much as possible. Herein, there exist two optimization variables Γ_k and θ_k, i.e., the *sequential* attack signal $\theta \triangleq \{\theta_0, \theta_1, \dots, \theta_N\}$ and *sequential* attack selection strategy $\Gamma \triangleq \{\Gamma_0, \Gamma_1, \dots, \Gamma_N\}$ where N is the given upper bound of finite-time iteration. Then, we construct the following optimization problem $\mathcal{P}_0$.

$$\begin{aligned} \mathcal{P}_{\mathbf{0}}: \quad & \min_{\{\theta,\Gamma\}} J = J_1 + J_2 \\ & \text{s.t. } (2), \end{aligned} \tag{3}$$

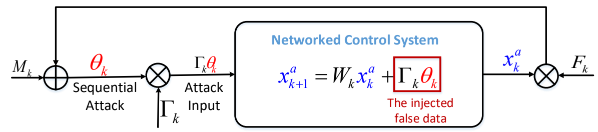


Fig. 1. The schematic of the optimal sequential attack design

where the sum of the state error J_1 and the energy of injected false data J_2 in finite time satisfy

$$\begin{cases} J_1 = \sum_{k=0}^{N} \left(\|x^a_k - x^*\|^2_{P_k} \right) + \|x^a_{N+1} - x^*\|^2_H, \\ J_2 = \sum_{k=0}^{N} \left(\|\Gamma_k \theta_k\|^2_{Q_k} \right), \end{cases}$$

and x^* is the expected malicious state predefined by the adversary and Q_k, P_k and H are the positive definite weight matrices, respectively.

The challenges of directly solving problem $\mathcal{P}_0$ result from the nonlinearity and non-convexity of the objective function J with respect to two closely coupled optimization variables Γ_k and θ_k. Furthermore, it is difficult to directly obtain the gradients of the objective function for variables θ and Γ to solve problem $\mathcal{P}_0$. If we can explore the relationship between the attack signal θ_k and the attack selection strategy Γ_k and derive an analytical closed-form relation, it is vital to simplify the solution of problem $\mathcal{P}_0$. Thus, we decompose $\mathcal{P}_0$ and first focus on problem $\mathcal{P}_1$:

$$\begin{aligned} \mathcal{P}_{\mathbf{1}}: \quad & \min_{\{\theta_0,\theta_1,\dots,\theta_N\}} J = J_1 + J_2 \\ & \text{s.t. } (2), \end{aligned} \tag{4}$$

where the attack selection strategy Γ is fixed. In an extended part of the paper, we will deal with Γ under the obtained optimal *sequential* attack signal θ. In this paper, we mainly tackle problem $\mathcal{P}_1$ and analyze the relationship between the injected attack signal θ and the attack selection strategy Γ.

III. OPTIMAL SEQUENTIAL ATTACK SCHEME

In this section, we solve problem $\mathcal{P}_1$ and derive the optimal sequential attack signal based on dynamic programming. Then, we excavate its critical parameters' property.

A. Attack Scheme Design

The schematic of the optimal sequential attack design is shown in Fig. 1. After giving the attack selection strategy Γ_k, the critical parameters F_k and M_k can be obtained backward offline based on (6) and (8). Then, the solution of problem $\mathcal{P}_1$, i.e., the optimal sequential attack θ_k is derived in the following theorem.

***Theorem** 1:* (Optimal Sequential Attack) The optimal sequential attack θ_k for $k = 0, 1, \cdots, N$, that minimizes J in (4) is

$$\theta_k = F_k x^a_k + M_k, \tag{5}$$

where

$$F_k = -R_k^{-1} \Gamma_k^{\mathrm{T}} K_{k+1} W_k, \tag{6}$$

with $R_k = \Gamma_k^{\mathrm{T}}(Q_k + K_{k+1})\Gamma_k$ and

$$K_k = P_k + W_k^{\mathrm{T}} K_{k+1} W_k + 2W_k^{\mathrm{T}} K_{k+1}\Gamma_k F_k + F_k^{\mathrm{T}}\Gamma_k^{\mathrm{T}}(Q_k + K_{k+1})\Gamma_k F_k, \tag{7}$$

and

$$M_k = \begin{cases} R_k^{-1}\Gamma_k^{\mathrm{T}} K_{k+1} x^*, k = N, \\ R_k^{-1}\Gamma_k^{\mathrm{T}} K_{k+1}(P_{k+1}x^* - W_{k+1}^{\mathrm{T}} K_{k+2}\Gamma_{k+1} M_{k+1}), k \neq N. \end{cases} \tag{8}$$

Proof: The proof can be completed by solving the Bellman equation backward from time $N+1$ of termination.

When time $k = N+1$, $K_{N+1} = H$, for any $x_{N+1}^a \in \mathbb{R}^n$, the value function

$$\begin{aligned} &V(x_{N+1}^a, N+1) \\ =&(x_{N+1}^a - x^*)^{\mathrm{T}} H (x_{N+1}^a - x^*) \\ =&(x_{N+1}^a)^{\mathrm{T}} K_{N+1}(x_{N+1}^a) + G_{N+1}, \end{aligned} \tag{9}$$

where $G_{N+1} = -2(x_{N+1}^a)^{\mathrm{T}} K_{N+1} x^* + \|x^*\|^2$. Note that the value function $V(x_{N+1}^a, N+1)$ is the quadratic function with respect to x_{N+1}^a. Next, with the mathematical induction method, we prove that the value function always satisfies the following form

$$V(x_{k+1}^a, k+1) = (x_{k+1}^a)^{\mathrm{T}} K_{k+1}(x_{k+1}^a) + G_{k+1}, \tag{10}$$

where K_k is the real symmetric positive definite matrix for $k = 0, 1, \ldots, N$.

Then, we derive the optimal attack signal θ_N at time N. With the obtained value function $V(x_{N+1}^a, N+1)$ in (9), for any $x_N^a \in \mathbb{R}^n$, we have

$$\begin{aligned} &V(x_N^a, N) \\ =&\min\nolimits_{\theta_N} \big\{(x_N^a - x^*)^{\mathrm{T}} P_N (x_N^a - x^*) \\ &+ \|\Gamma_N \theta_N\|_{Q_N}^2 + V(x_{N+1}^a, N+1)\big\} \\ =&\min\nolimits_{\theta_N} \big\{(x_N^a - x^*)^{\mathrm{T}} P_N (x_N^a - x^*) \\ &+ \theta_N^{\mathrm{T}}\Gamma_N^{\mathrm{T}} Q_N \Gamma_N \theta_N + G_{N+1} \\ &+ (W_N x_N^a + \Gamma_N\theta_N)^{\mathrm{T}} K_{N+1}(W_N x_N^a + \Gamma_N \theta_N)\big\}. \end{aligned} \tag{11}$$

Taking the derivative of (11) with respect to θ_N, for any $x_N^a \in \mathbb{R}^n$, we have $2\theta_N^{\mathrm{T}}\Gamma_N^{\mathrm{T}} Q_N \Gamma_N + 2(W_N x_N^a + \Gamma_N\theta_N)^{\mathrm{T}} K_{N+1}\Gamma_N = 0$. Thus, it can be inferred that

$$\theta_N = -R_N^{-1}(\Gamma_N^{\mathrm{T}} K_{N+1} W_N x_N^a - \Gamma_N^{\mathrm{T}} K_{N+1} x^*), \tag{12}$$

where $R_N \triangleq \Gamma_N^{\mathrm{T}}(Q_N + K_{N+1})\Gamma_N$. (12) is rewritten as

$$\theta_N = F_N x_N^a + M_N, \tag{13}$$

where $F_N = -[\Gamma_N^{\mathrm{T}}(Q_N + K_{N+1})\Gamma_N]^{-1}\Gamma_N^{\mathrm{T}} K_{N+1} W_N$ and $M_N = [\Gamma_N^{\mathrm{T}}(Q_N + K_{N+1})\Gamma_N]^{-1}\Gamma_N^{\mathrm{T}} K_{N+1} x^*$.

When time $k = N$, combined with (11) and (13), we derive the value function

$$\begin{aligned} &V(x_N^a, N) \\ =& (x_N^a)^{\mathrm{T}} \big\{P_k + W_k^{\mathrm{T}} K_{K+1} W_k + 2W_k^{\mathrm{T}} K_{k+1}\Gamma_k F_k \\ &+ F_k^{\mathrm{T}}\Gamma_k^{\mathrm{T}}(Q_k + K_{k+1})\Gamma_k F_k\big\} (x_N^a) + G_{N+1} \\ &- 2(x^*)^{\mathrm{T}} P_N x_N^a + \|x^*\|^2 \\ &+ \theta_N^{\mathrm{T}}\Gamma_N^{\mathrm{T}}(Q_N + K_{N+1})\Gamma_N\theta_N \\ &+ 2x_N^{\mathrm{T}} W_N^{\mathrm{T}} K_{N+1}\Gamma_N M_N. \end{aligned} \tag{14}$$

Let

$$\begin{aligned} K_N \triangleq& P_N + W_N^{\mathrm{T}} K_{N+1} W_N + 2W_N^{\mathrm{T}} K_{N+1}\Gamma_N F_N \\ &+ F_N^{\mathrm{T}}\Gamma_N^{\mathrm{T}}(Q_N + K_{N+1})\Gamma_N F_N \end{aligned}$$

and

$$\begin{aligned} G_N \triangleq& G_{N+1} - 2(x^*)^{\mathrm{T}} P_N x_N^a + 2x_N^{\mathrm{T}} W_N^{\mathrm{T}} K_{N+1}\Gamma_N M_N \\ &+ \theta_N^{\mathrm{T}}\Gamma_N^{\mathrm{T}}(Q_N + K_{N+1})\Gamma_N\theta_N + \|x^*\|^2. \end{aligned}$$

Thus, the value function $V(x_N^a, N)$ also satisfies (10).

Then, we derive the optimal attack signal θ_{N-1} at time $N-1$. With the obtained value function $V(x_N^a, N)$ in (9), for any $x_{N-1}^a \in \mathbb{R}^n$, we have

$$\begin{aligned} &V(x_{N-1}^a, N-1) \\ =& \min\nolimits_{\theta_{N-1}} \big\{(x_{N-1}^a - x^*)^{\mathrm{T}} P_{N-1}(x_{N-1}^a - x^*) \\ &+ \|\Gamma_{N-1}\theta_{N-1}\|_{Q_{N-1}}^2 + V(x_N^a, N)\big\} \\ =& \min\nolimits_{\theta_{N-1}} \big\{(x_{N-1}^a - x^*)^{\mathrm{T}} P_{N-1}(x_{N-1}^a - x^*) \\ &+ \theta_{N-1}^{\mathrm{T}}\Gamma_{N-1}^{\mathrm{T}} Q_{N-1}\Gamma_{N-1}\theta_{N-1} \\ &+ (W_{N-1}x_{N-1}^a + \Gamma_{N-1}\theta_{N-1})^{\mathrm{T}} \\ &K_N(W_N x_{N-1}^a + \Gamma_{N-1}\theta_{N-1}) + G_N\big\}. \end{aligned} \tag{15}$$

Taking the derivative of (15) with respect to θ_{N-1}, for any $x_{N-1}^a \in \mathbb{R}^n$, we have $2\theta_{N-1}^{\mathrm{T}}\Gamma_{N-1}^{\mathrm{T}} Q_{N-1}\Gamma_{N-1} + 2(W_{N-1}x_{N-1}^a + \Gamma_{N-1}\theta_{N-1})^{\mathrm{T}} K_N \Gamma_{N-1} = 0$. Thus, it can be inferred that

$$\begin{aligned} \theta_{N-1} =& -R_{N-1}^{-1}(\Gamma_{N-1}^{\mathrm{T}} K_N W_{N-1} x_{N-1}^a \\ &- \Gamma_{N-1}^{\mathrm{T}} K_N P_N x^* + W_N^{\mathrm{T}} K_{N+1}\Gamma_N M_N), \end{aligned} \tag{16}$$

which also can be derived as $\theta_{N-1} = F_{N-1}x_{N-1}^a + M_{N-1}$ with $F_{N-1} = -R_{N-1}^{-1}\Gamma_{N-1}^{\mathrm{T}} K_N W_{N-1}$ and

$$M_{N-1} = R_{N-1}^{-1}\Gamma_{N-1}^{\mathrm{T}} K_N(P_N x^* - W_N^{\mathrm{T}} K_{N+1}\Gamma_N M_N).$$

When time $k = N-1$, combined (15) with (16), we derive the value function

$$V(x_{N-1}^a, N-1) = (x_{N-1}^a)^{\mathrm{T}} K_{N-1}(x_{N-1}^a) + G_{N-1},$$

where

$$\begin{aligned} K_{N-1} =& P_{N-1} + W_{N-1}^{\mathrm{T}} K_N W_{N-1} + 2W_{N-1}^{\mathrm{T}} K_N \Gamma_{N-1} F_{N-1} \\ &+ F_{N-1}^{\mathrm{T}}\Gamma_{N-1}^{\mathrm{T}}(Q_{N-1} + K_N)\Gamma_{N-1}F_{N-1} \end{aligned}$$

and

$$\begin{aligned} G_{N-1} =& G_N - 2(x^*)^{\mathrm{T}} P_{N-1} x_{N-1}^a \\ &+ \|x^*\|^2 + \theta_{N-1}^{\mathrm{T}}\Gamma_{N-1}^{\mathrm{T}}(Q_{N-1} + K_N)\Gamma_{N-1}\theta_{N-1} \\ &+ 2x_{N-1}^{\mathrm{T}} W_{N-1}^{\mathrm{T}} K_N \Gamma_{N-1} M_{N-1}. \end{aligned}$$

Continue the iterative process for $k = 0, 1, \ldots, N-2$. Finally, we can obtain the optimal sequential attack signal

$$\theta_k = F_k x_k^a + M_k,$$

and the value function

$$V(x_{k+1}^a, k+1) = (x_{k+1}^a)^{\mathrm{T}} K_{k+1}(x_{k+1}^a) + G_{k+1},$$

Thus, the proof is completed. ■

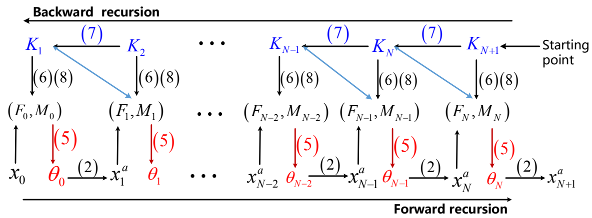


Fig. 2. The recursion flow of F_k, K_k, M_k and θ_k

Theorem 1 reveals the strongly coupled relationship between the optimal sequential attack signal and the attack selection strategy. Especially, the optimal attack signal θ_k at time k is the function of the system state x_k^a. Besides, it is related to the system structure W_k, the expected malicious state x^*, and the initial states x_0. In other words, once the adversary knows the initial state x_0 and the system structure W_k, the optimal sequential attack signal θ_k can be designed after the adversary determines the expected malicious state x^*, the attack selection strategy Γ_k, and weight matrices P_k, Q_k and H. As shown in Fig. 2, with the initial matrix K_{N+1}, F_k, K_k and M_k are derived backward based on (6), (7) and (8), respectively. Then, with the known initial states x_0 and (5), the adversary can directly inject optimal sequential attack signal θ_k along the iteration timeline.

B. Property Analysis

In this part, we demonstrate the inverse convergence of the critical parameter matrix K_k in (7) and vector F_k in (6), respectively. Since K_k and F_k are derived backward, its inverse convergence is defined as follows.

Definition 2: (Inverse Convergence) Matrix/Vector/Point convergence is called inverse convergence if the matrix/vector/point is derived backward and converges in the reverse order of iteration time.

Based on Definition 2, we find that the sequential $\{K_N, K_{N-1}, K_{N-2}, \ldots, K_2, K_1\}$ and $\{F_N, F_{N-1}, F_{N-2}, \ldots, F_1, F_0\}$ converge forward, which are also called inverse convergence of K_k and F_k. With this property, it is possible to quickly obtain the steady-state parameters K_k and F_k. In other words, only a small number of iteration time k are required to derive F_k and K_k backward regardless of the finite-time N. Based on these few backward recursions, the optimal sequential attack signal can be directly designed.

In what follows, we first analyze the symmetry and positive definiteness of K_k, and the system's finite-time stability, which is beneficial to proving its inverse convergence.

***Lemma** 1 (Symmetry and positive definiteness of K_k):* The matrix K_k in (7) is a positive definite Hermitian matrix for $k = 0, 1, \ldots, N$, i.e., $K_k = K_k^* \succ 0$.

Proof: The proof can be divided into two parts. One is to show the Hermitian matrix K_k. The other is to show $K_k \succ 0$. Both are based on mathematical induction method. The concrete proof can be founded in [15]. ■

Corollary 1: K_k in (7) can be simplified as

$$K_k = P_k + W_k^{\mathrm{T}} K_{k+1} W_k - R_k^{-1} W_k^{\mathrm{T}} K_{k+1} \Gamma_k \Gamma_k^{\mathrm{T}} K_{k+1} W_k.$$

Proof: The proof can be founded in [15]. ■

***Lemma** 2 (Finite-time stability):* Consider a discrete-time system with a corresponding positive definite matrix-valued Lyapunov function $\tilde{V} : \mathbb{R}^{n\times n} \to \mathbb{R}$ and let $\tilde{V}_k = \tilde{V}(K_k - K^\star)$. Let α and ϵ be a constant in the open interval $(0, 1)$. Let $\tilde{V}_N > 0$ be the finite initial value of the Lyapunov function with respect to K_k. Denote $\varphi_k \triangleq \varphi(\tilde{V}_k^{1-\alpha})$ where $\varphi : \mathbb{R}^+ \to \mathbb{R}^+$ is a class-$\mathcal{K}$ function of $\tilde{V}_k^{1-\alpha}$ that satisfies

$$\frac{\varphi_k}{\varphi_N} \geq 1 - \epsilon \quad \text{for} \quad \tilde{V}_k^{1-\alpha} \in (\tilde{V}_N^{1-\alpha} - \chi, \tilde{V}_N^{1-\alpha}) \tag{17}$$

for some finite positive constant $\chi < \tilde{V}_N^{1-\alpha}$. Then, if $\tilde{V}_k$ satisfies the relation

$$\tilde{V}_{k-1} - \tilde{V}_k = -\varphi_k \tilde{V}_k^\alpha, \tag{18}$$

matrix K_k has the steady state and converges to $K^\star$ for $0 \leq k < \xi^\star$ where the positive integer $\xi^\star$ satisfies (20).

Proof: Note that (18) is a sufficient condition to ensure that $\tilde{V}_{k-1} - \tilde{V}_k$ decreases along the convergence direction of matrix $K_k - K^\star$ in the discrete-time system. Moreover, given φ_k in (17), if and only if $\tilde{V}_k = 0$, the equality will be zero. Then, (18) can be expressed as

$$\tilde{V}_{k-1} = \tilde{V}_k - \varphi_k \tilde{V}_k^\alpha = \tilde{V}_k\left(1 - \frac{\varphi_k}{\tilde{V}_k^{1-\alpha}}\right).$$

Let the initial value of the Lyapunov function be

$$\tilde{V}_N = \beta_N (\varphi_N)^{\frac{1}{1-\alpha}},\ \beta_N > 0.$$

Substituting the value $\tilde{V}_N$ in (18), one gets

$$\tilde{V}_{N-1} = \beta_N (\varphi_N)^{\frac{1}{1-\alpha}} - \varphi_N \tilde{V}_N^\alpha = (\beta_N - \beta_N^\alpha)(\varphi_N)^{\frac{1}{1-\alpha}}.$$

Define $\beta_{N-1} = \beta_N - \beta_N^\alpha$. Then we have $\tilde{V}_{N-1} = \beta_{N-1} - \beta_{N-1}^\alpha$. Substituting the above value $\tilde{V}_{N-1}$ into (18), it can be inferred that

$$\tilde{V}_{N-2} = \beta_{N-2}(\varphi_N)^{\frac{1}{1-\alpha}},$$

where $\beta_{N-2} = \beta_{N-1} - a_{N-1}\beta_{N-1}^\alpha$ and $a_{N-1} = \frac{\varphi_{N-1}}{\varphi_N}$. Similarly, with a recursive relation of β_k for $1 \leq k \leq N$, $\tilde{V}_{k-1}$ can be expressed as

$$\tilde{V}_{k-1} = \beta_{k-1}(\varphi_N)^{\frac{1}{1-\alpha}}, \tag{19}$$

where $\beta_{k-1} = \beta_k - a_k \beta_k^\alpha$ and $a_k = \frac{\varphi_k}{\varphi_N}$. If $\tilde{V}_k$ and φ_k satisfy (17), then we obtain

$$\begin{aligned}\beta_{k-1} \leq& \beta_k - (1-\epsilon)\beta_k^\alpha,\\ =& \epsilon\beta_k^\alpha - (1 - \beta_k^{1-\alpha})\beta_k^\alpha.\end{aligned}$$

Since $\tilde{V}_{k-1} = \tilde{V}(K_{k-1} - K^\star)$ is positive definite, β_{k-1} is non-negative. When $\beta_{k-1} = 0$, it follows that

$$\epsilon = 1 - \beta_k^{1-\alpha} \Leftrightarrow \beta_k^{1-\alpha} = 1 - \epsilon. \tag{20}$$

Let $k = \xi^\star$ be the smallest integer for which (20) is satisfied, i.e., $\beta_{\xi^\star} = (1-\epsilon)^{\frac{1}{1-\alpha}}$. In other words, $\beta_{\xi^\star - 1} = 0$. Thus, it is easy to obtain that $\tilde{V}_k = 0$ with $\beta_k = 0$ for $0 \leq k < \xi^\star$. Consequently, K_k converges to $K^\star$ inversely in finite-time $\xi^\star$. The proof is completed. ■

Lemma 2 provides a new insight to prove the finite-time inverse convergence for the matrix K_k in (7), which is also an extension of finite-time vector forward convergence [16] to matrix inverse convergence. Based on Lemma 2, then we develop a matrix-valued Lyapunov function in the following theorem to show the inverse convergence of K_k.

***Theorem** 2 (Finite-time inverse convergence of K_k):* Let $\xi^\star$ be the smallest integer for the inverse convergence of matrix K_k. The parameter matrix K_k in (7) converges inversely when $0 \leq k < \xi^\star$ where $\xi^\star$ satisfies (20).

Proof: The proof is completed by utilizing discrete-time Lyapunov analysis. With Corollary 1 and Lemma 2, we just need to find a Lyapunov function $\tilde{V}_k$, which satisfies the convergence condition in (18). The concrete proof can be founded in [15]. ■

From Theorem 2, we know that the inverse convergence of K_k for $k = 1, \ldots, N$ is independent of the initial matrix K_{N+1}. Furthermore, the inverse convergence of F_k is shown as follows.

Corollary 2 (Inverse Convergence of F_k): When the system structure W_k is fixed, the parameter vector F_k in (6) converges inversely when $0 \leq k < \xi^\star + 1$.

Proof: Since $F_k = -R_k^{-1}\Gamma_k^{\mathrm{T}} K_{k+1} W_k$ with $R_k = \Gamma_k^{\mathrm{T}}(Q_k + K_{k+1})\Gamma_k$ and K_k in (7), the proof can be completed if the convergence of K_{k+1} is guaranteed. When $0 \leq k < \xi^\star$, K_k converges inversely. Thus, F_k converges when $0 \leq k < \xi^\star + 1$. The proof is completed. ■

IV. Simulation Results

In this section, we evaluate the performance of the optimal sequential attack strategy, i.e., we analyze the driving performance and the inverse convergence of its critical parameters K_k and F_k.

Consider a consensus process with three agents. Under attacks, the dynamics of the whole system satisfy (1). We set the matrix $W = I_3 - 0.2 * L$, which can achieve the average consensus without attacks. Meanwhile, the system is stable and controllable. In the linear network, the Laplacian matrix $L = [1\ \ -1\ 0; -1\ 2\ \ -1; 0\ \ -1\ 1]$ and $L = [2\ \ -1\ \ -1; -1\ 2\ \ -1; -1\ \ -1\ 2]$ in the circle network. Let time $N = 50$, and weight matrices $P_k = Q_k = H = I_3$ for all $0 \leq k \leq N$. We set the initial state $x_0 = [-1\ 12\ -5]^{\mathrm{T}}$ and the expected malicious state $x^* = [0\ 0\ 0]^{\mathrm{T}}$.

1) Effects of the sequential attack signal θ on the system states: Given the attack selection strategy $\Gamma_1 = [1\ 0\ 0]^{\mathrm{T}}$ and the linear network, the differences between the states without attacks and that with the injected attack signal θ are shown in Fig. 3(a). It is illustrated that the injected sequential attack signal can steer the average consensus value $[2\ 2\ 2]^{\mathrm{T}}$ to the desired malicious state $x^* = [0\ 0\ 0]^{\mathrm{T}}$.

2) Effects of the attack selection strategy Γ on θ under different networks: We set attack selection strategy $\Gamma_1 = [1\ 0\ 0]^{\mathrm{T}}$, $\Gamma_2 = [0\ 1\ 0]^{\mathrm{T}}$, and $\Gamma_3 = [0\ 0\ 1]^{\mathrm{T}}$. The effects of different attack selection strategies on the injected sequential attack signal under linear and cycle networks are shown in Fig. 3(b). Notably, the injected sequential attack signal θ varies with the distinct attack selection strategies and approaches zero. Moreover, from Table I and Table II, we find that there exists a trade-off between the injected attack energy and the value of the objective function regardless of the type of the connected network. Specifically, the more the objective function needs to be minimized while driving the states to the malicious states, the more attack energy needs to be injected.

TABLE I

Results of different attack selection in linear networks

Network structure	Attack selection strategy Γ	Attack energy $\sum_{k=0}^{N} \theta_k^{\mathrm{T}} \theta_k$	**Objective function** J
Linear	$[1\ 0\ 0]^{\mathrm{T}}$	6.8787	238.6639
	$[0\ 1\ 0]^{\mathrm{T}}$	14.7073	206.0239
	$[0\ 0\ 1]^{\mathrm{T}}$	3.0517	300.6101

TABLE II

Results of different attack selection in circle networks

Network structure	Attack selection strategy Γ	Attack energy $\sum_{k=0}^{N} \theta_k^{\mathrm{T}} \theta_k$	**Objective function** J
Circle	$[1\ 0\ 0]^{\mathrm{T}}$	5.9828	234.0186
	$[0\ 1\ 0]^{\mathrm{T}}$	14.7073	193.3255
	$[0\ 0\ 1]^{\mathrm{T}}$	4.9348	242.1756

3) Effects of the initial states on θ: We set two types of initial states $x_0^{(1)} = [-1\ 12\ -5]^{\mathrm{T}}$ and $x_0^{(2)} = [-1\ 10\ -15]^{\mathrm{T}}$, and remain the other conditions. The effects of the initial states on the injected optimal sequential attack signal θ are shown in Fig. 3(c). It is illustrated that the size of the injected attack signal highly depends on the initial states. Even though there exists the same initial state for agent 1, the size of the injected attack signal is different and influenced by the initial states of other agents.

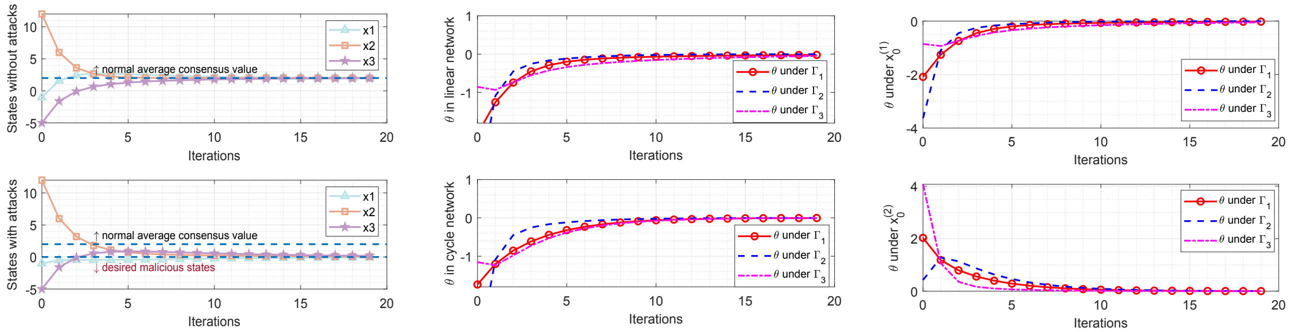
4) Inverse convergence of K_k and F_k: In this part, we show the inverse convergence of K_k and F_k, which are measured by the following index

$$K_c = \|K_k - K^\star\|, \tag{21}$$

and

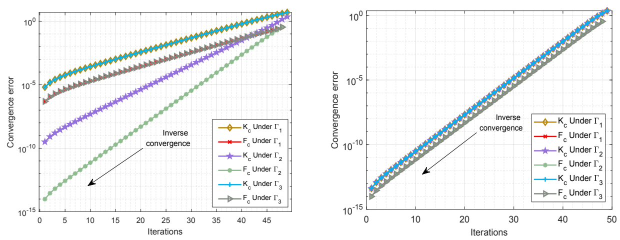
$$F_c = \|F_k - F^\star\|, \tag{22}$$

where $K^\star$ and $F^\star$ are the steady-state matrix of K_k and F_k for $0 \leq k \leq N$, respectively. Given the attack selection strategy $\Gamma_1 = [1\ 0\ 0]^{\mathrm{T}}$ and the other same conditions as the first part, the convergence error of K_k and F_k are illustrated as Fig. 4(a) and Fig. 4(b). Under the linear network, when the first or the third agent is compromised, the convergence error of K_k and F_k are the same, which is different from that when the only second agent is attacked. In other words, the effects of attack selection strategies on the injected attack signal depend on the network structure. Especially, under the cycle network, the selection of the compromised agents does not affect the injected signal. Moreover, comparing Fig. 4(a) with Fig. 4(b), it is easy to reveal that the convergence



(a) The variations of states with/without attacks (b) Effects of Γ on θ under different networks (c) Effects of x_0 on θ under the cycle network

Fig. 3. Performance of the optimal sequential attack signal.



(a) Linear network (b) Cycle network

Fig. 4. The convergence error of K_k and F_k under different networks.

rate of F_k is greater than that of K_k, which is owing to the convergence of weight matrix W_k. From Table III, we show the inverse convergence times for K_k and F_k, which validate the result in Corollary 2. Meanwhile, we find that only 15 iteration times are required to compute K_k and 14 iteration times for F_k regardless of the length of N.

TABLE III
TIMES OF INVERSE CONVERGENCE OF K_k AND F_k

Length of N	50	100	200	1000
Inverse Convergence Time of K_k	$[1, 35]$	$[1, 85]$	$[1, 185]$	$[1, 985]$
Inverse Convergence Time of F_k	$[1, 36]$	$[1, 86]$	$[1, 186]$	$[1, 186]$

V. CONCLUSION

We investigated the relationship between the injected attack signal and the attack selection strategy. Specifically, we first designed a sequential attack scheme where the injected attack signals vary with the sampling time in discrete-time systems. Then, we derived the optimal sequential attack signal where the adversary steers the system state to the malicious one, which reveals the strongly coupled relationship about the attack selection strategy. When the adversary knows the knowledge of the system model and clears the expected malicious state, the designed optimal sequential attack signal is related to the initial state and the attack selection strategy. In addition, we proved the inverse convergence of the critical parameters in the optimal sequential attack signal. Future work will strive to obtain the near-optimal attack selection strategy under the proposed optimal sequential attack signal.

REFERENCES

[1] 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.

[2] X. Luo, C. Fang, J. He, C. Zhao, and D. Paccagnan, "A feedback-optimization-based model-free attack scheme in networked control systems," *arXiv preprint arXiv:2212.07633*, 2022.

[3] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM TISSEC*, vol. 14, no. 1, pp. 1–33, 2011.

[4] T. Sui, Y. Mo, D. Marelli, X. Sun, and M. Fu, "The vulnerability of cyber-physical system under stealthy attacks," *IEEE Transactions on Automatic Control*, vol. 66, no. 2, pp. 637–650, 2020.

[5] 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.

[6] C. Fang, Y. Qi, P. Cheng, and W. X. Zheng, "Optimal periodic watermarking schedule for replay attack detection in cyber–physical systems," *Automatica*, vol. 112, p. 108698, 2020.

[7] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 635–646, 2020.

[8] Y. Chen, S. Kar, and J. M. Moura, "Cyber-physical attacks with control objectives," *IEEE Transactions on Automatic Control*, vol. 63, no. 5, pp. 1418–1425, 2017.

[9] Y.-G. Li and G.-H. Yang, "Optimal stealthy false data injection attacks in cyber-physical systems," *Information Sciences*, vol. 481, pp. 474–490, 2019.

[10] M. Jafari, M. A. Rahman, and S. Paudyal, "Optimal false data injection attacks against power system frequency stability," *IEEE Transactions on Smart Grid*, 2022.

[11] G. Wu, J. Sun, and J. Chen, "Optimal data injection attacks in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 48, no. 12, pp. 3302–3312, 2018.

[12] L. Ye, N. Woodford, S. Roy, and S. Sundaram, "On the complexity and approximability of optimal sensor selection and attack for kalman filtering," *IEEE Transactions on Automatic Control*, vol. 66, no. 5, pp. 2146–2161, 2020.

[13] X. Luo, C. Zhao, C. Fang, and J. He, "Submodularity-based false data injection attack scheme in multi-agent dynamical systems," in *IEEE ACC*, 2022, pp. 4998–5003.

[14] 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.

[15] X. Luo, C. Fang, C. Zhao, P. Cheng, and J. He, "Optimal sequential false data injection attack scheme: Finite-time inverse convergence," [Online].Available:https://iwin-fins.com/wp-content/uploads/2023/08/23CDCluo.pdf, 2023.

[16] R. Hamrah, A. K. Sanya, and S. P. Viswanathan, "Discrete finite-time stable position tracking control of unmanned vehicles," in *IEEE CDC*, 2019, pp. 7025–7030.