Completely Stealthy FDI Attack Against State Estimation in Networked Control Systems

Yifa Liu, *Student Member, IEEE*, and Long Cheng, *Senior Member, IEEE*

***Abstract*—An effective false data injection attack should cause enough damage to the system while avoiding being spotted by detection methods. This brief proposes an extremely stealthy attack strategy, which can make the residual almost always unchanged to invalidate both the widely used χ^2 detector and the advanced summation detector and can eventually cause unbound state deviations. Compared with the existing attack methods, the proposed attack strategy can reduce the sum of cumulative residual increments by 85.39% while causing 9817001 times of the state deviations in the numerical simulations.**

***Index Terms*—False data injection attack, estimation, complete stealthiness, detection, networked control systems.**

I. Introduction

BENEFITED from the advances in technologies, such as sensing, communication, computation and control, large-scale networked control systems (NCSs) emerge and significantly improve efficiency [1]. NCSs are applicable in many fields including but not limited to smart transportation [2], water supply [3], and electricity and electronics systems [4]. However, NCSs are proven vulnerable to cyber attacks due to the addition of unreliable communications [5]. There are two common categories of cyber attacks: denial-of-service (DoS) attacks [6] and false data injection (FDI) attacks [7], [8]. False data injection attacks tamper with control and/or measurement data without obstructing channel operation and are therefore more difficult to be detected [9]. Due to the stealthiness, FDI attacks are more destructive and dangerous [10].

To combat FDI attacks, it needs to detect the attack first. Many studies about detecting attacks, especially early ones, used static detection methods [11], [12], [13], which were proven to be vulnerable and have serious defects [14]. Therefore, more dynamic detection methods were applied, such as the widely used χ^2 detector [15] and Kullback-Leibler divergence (KLD) detector [16]. The necessary and sufficient conditions of stealthy FDI attacks against χ^2 detector for causing infinite estimation errors were investigated in [17], [18]. And based on those conditions, attack sequences can be designed to bypass the χ^2 detector. A novel data-driven FDI attack method and the necessary and sufficient design conditions for achieving complete stealthiness against the KLD detector were proposed in [19], in which a good attack effect can be achieved without precise parameters. Since the χ^2 detector and the KLD detector are based on single-step information, the attacker can launch long-term attacks causing only a small fluctuation at each time to achieve attack goals.

Then, a summation (SUM) detector taking the cumulative information as the indicator was developed to counter those well-constructed attack methods in [20]. Through the comprehensive examination of historical information, this advanced SUM detector can spot those attacks splitting magnitude in time domain. In recent years, an attack strategy with energy stealthiness was proposed in [21], which can gradually remove the perturbations to fool the SUM detector. However, this attack strategy still caused short-term exposure risks and took effect more slowly. Then, a natural question is whether there is an attack strategy that can completely hide its trace and cause significant harm rapidly.

Motivated by this idea, this brief proposes an attack strategy with ultimate stealthiness in terms of the SUM detector and theoretically other historical information based detectors. This attack strategy can directly make the residual be zero after the second step, instead of making the residual asymptotically approach zero. Furthermore, the proposed attack strategy can rapidly cause more state deviations in the early stages and eventually cause infinite state deviations to NCSs. Numerical simulations indicate that the proposed method can achieve better attack performance in both stealthiness and damage compared with other attack strategies.

Notation: $\mathbf{0}$, I, and $\mathbf{O}$ denote the vector with all zeros, the identity matrix, and the matrix with all zeros with appropriate sizes, respectively. $\mathbf{e}_i$ denotes the i-th column of I.

II. Preliminaries

This section describes the control models of NCSs and the corresponding FDI attacks against measurements.

A. Control System Model

Consider a sampled-data based NCS described by the following stochastic linear state-space equation

$$\begin{cases} x_{k+1} = Ax_k + Bu_k + w_k, \\ y_k \quad\;\; = Hx_k + v_k, \end{cases} \tag{1}$$

Manuscript received 6 October 2022; accepted 17 October 2022. Date of publication 26 October 2022; date of current version 6 March 2023. This work was supported in part by the National Natural Science Foundation of China under Grant 62025307 and Grant U1913209, and in part by the Beijing Natural Science Foundation under Grant JQ19020. This brief was recommended by Associate Editor J. Xie. *(Corresponding author: Long Cheng.)*

Yifa Liu is with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China, and also with the School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing 100049, China.

Long Cheng is with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190, China, also with the School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing 100049, China, and also with the Department of Mathematics and Theories, Peng Cheng Laboratory, Shenzhen 518055, China (e-mail: long.cheng@ia.ac.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TCSII.2022.3217132.

Digital Object Identifier 10.1109/TCSII.2022.3217132

where $x_k \in \mathbb{R}^n, y_k \in \mathbb{R}^m, u_k \in \mathbb{R}^p$ are the state, the measurement, and the input at the k-th time step, respectively; $w_k \sim N_n(\mathbf{0}, Q)$, $v_k \sim N_m(\mathbf{0}, R)$, $\{w_i\}$ and $\{v_i\}$ are mutual independent i.i.d noises, $R \in \mathbb{R}^{m\times m}$ and $Q \in \mathbb{R}^{n\times n}$ are both positive definite symmetric matrices. It is assumed that $(A,\ B)$ is stabilizable and (H, A) is observable.

Assumption 1: A has at least one eigenvalue λ with the maximum modulus satisfying $|\lambda| > 1$.

In order to stabilize system (1) and maintain its normal operation, the following feedback control is adopted

$$u_k = K\hat{x}_k, \tag{2}$$

where $K \in \mathbb{R}^{p\times n}$ is the control gain, $\rho(A + BK) < 1$, $\rho(\cdot)$ denotes the spectral radius, and $\hat{x}_k$ is the estimated state.

B. State Estimation

Since it is difficult and non-economic to directly obtain all system states in massive NCSs, the estimated states are used instead. The methods to acquire the state estimation include static methods and dynamic methods. Many electricity and electronics systems adopt static estimation methods. The most commonly used static method is the weighted least square (WLS) method, in which the estimated states are

$$\hat{x}_k^s = (H^T RH)^{-1} H^T R y_k, \tag{3}$$

in order to minimize $J_k = (y_k - H\hat{x}_k^s)^T R^{-1}(y_k - H\hat{x}_k^s)$. And the corresponding estimation residual r_k^s is defined as

$$r_k^s = y_k - H\hat{x}_k^s = [I - H(H^T RH)^{-1} H^T R]y_k. \tag{4}$$

The static estimated state and its corresponding residual entirely rely on the current measurement, resulting in static methods easier to be compromised [22].

Most control systems are more inclined to adopt dynamic estimation methods and the following observer is used

$$\begin{cases} \hat{x}_{k+1} &= A\hat{x}_k + Bu_k + Lr_{k+1}, \\ r_{k+1} &= y_{k+1} - H(A\hat{x}_k + Bu_k), \\ e_k &= x_k - \hat{x}_k, \end{cases} \tag{5}$$

where $r_k \in \mathbb{R}^m$ and $e_k \in \mathbb{R}^n$ are the residual and the estimation error, respectively, and $L \in \mathbb{R}^{n\times m}$ is the observer gain matrix satisfying $\rho(A - LHA) < 1$.

In this brief, attacks against both static and dynamic estimation based detection methods are studied.

C. FDI Attacks Against Measurements

The estimation relies on the data from the remote distributed sensors, which are far away from the central management and lack sufficient protection. The attacker can launch an FDI attack against those defenseless sensors to tamper with the measurement data, and the tampered measurement becomes

$$y_k^\alpha = Hx_k + v_k + \alpha_k, \tag{6}$$

where $y_k^\alpha \in \mathbb{R}^m$ and $\alpha_k \in \mathbb{R}^m$ are the tampered measurement and the additive attack vector, respectively. In this brief, the symbols with superscript α denote the corresponding variables after the attack. Then the entire closed-loop system without attack and that under attacks can be derived as follows

$$\begin{cases} x_{k+1} &= Ax_k + BK\hat{x}_k + w_k \\ y_k &= Hx_k + v_k \\ \hat{x}_{k+1} &= (A + BK)\hat{x}_k + Lr_{k+1} \\ r_k &= y_k - H(A + BK)\hat{x}_{k-1} \\ e_{k+1} &= (A - LHA)e_k + (I - LH)w_k - Lv_{k+1}, \end{cases} \tag{7}$$

$$\begin{cases} x_{k+1}^\alpha &= Ax_k^\alpha + BK\hat{x}_k^\alpha + w_k \\ y_k^\alpha &= Hx_k^\alpha + v_k + \alpha_k \\ \hat{x}_{k+1}^\alpha &= (A + BK)\hat{x}_k^\alpha + Lr_{k+1}^\alpha \\ r_k^\alpha &= y_k^\alpha - H(A + BK)\hat{x}_{k-1}^\alpha \\ e_{k+1}^\alpha &= (A - LHA)e_k^\alpha + (I - LH)w_k - Lv_{k+1} - L\alpha_{k+1}. \end{cases} \tag{8}$$

The first attack occurs at the first time step, *i.e.,* $\alpha_t = \mathbf{0}$, $\forall t \le 0$. The symbols with Δ denote the increments, namely the difference between the corresponding variables of these two systems, *i.e.,* $\Delta x_k = x_k^\alpha - x_k$. Under this setting, the initial values are $[x_0\ y_0\ \hat{x}_0\ r_0]^T = [x_0^\alpha\ y_0^\alpha\ \hat{x}_0^\alpha\ r_0^\alpha]^T$.

D. Detection and Stealthiness

To combat attackers, the control center needs to detect malicious attacks. From (7) and (8), the attack directly changes the residual (and measurement), therefore, the residual r or its variants are selected as the test statistics in most detection methods, such as the χ^2 detector and the SUM detector.

Definition 1: The FDI attack is the unbounded attack if $\lim_{t\to\infty} \|\Delta e_t\| = \infty$.

The χ^2 detector is a widely used detector whose indicator is

$$g_k^{\chi^2} = r_k^T P^{-1} r_k \lesseqgtr g, \tag{9}$$

where P is a positive definite matrix and g is the threshold. If $g_k^{\chi^2} > g$, an alarm is triggered.

Definition 2 [17], [18]: The FDI attack has stealthiness if there exists a constant γ such that $\|\Delta r_t\| \le \gamma,\ \forall t > 0$.

From Definition 2, the attack with stealthiness can bypass the χ^2 detector. Then, the following SUM detector is proposed to counter those attacks with stealthiness [20],

$$g_k^{SUM} = \frac{1}{k}\Big(\sum_{i=1}^{k} r_i^T\Big) P^{-1} \Big(\sum_{i=1}^{k} r_i\Big) \lesseqgtr g, \tag{10}$$

where P and g are the same as those in (9).

Definition 3 [21]: The FDI attack has "complete stealthiness" if there exists a constant γ such that $\|\Delta r_t\| \le \gamma, \forall t > 0$ and $\lim_{t\to\infty} \|\Delta r_t\| = 0$.

This condition can ensure the convergence of residual increments and then the sum of residual increments is bounded to bypass the SUM detection. However, "complete stealthiness" only requires the limit of the residual increment to be zero. Then a natural question is whether it can be found an absolutely strict condition requiring the residual increment to be zero almost every step.

Based on this motivation, this brief proposes the following more stringent stealthiness requirements.

Definition 4: The FDI attack has complete stealthiness if there exist constants γ and T such that $\|\Delta r_t\| \le \gamma, \forall 0 < t \le T$ and $\|\Delta r_t\| = 0,\ \forall t > T$.

This definition ensures that the residual increment is zero after time T, and therefore, the residual under attack is always

the same as that if there is no attacks. In this brief, the time limit T is set to be 2 (the low bound).

Then, the main purpose of this brief is to achieve the following objective:

Objective 1: Find an attack sequence $\{\alpha_1, \alpha_2, \cdots\}$ such that $\|\Delta r_1\| \leq \gamma$, $\gamma > 0$, $\|\Delta r_t\| = 0$, $\forall t \geq 2$, $\lim_{t\to\infty} \|\Delta e_t\| = \infty$.

III. Main Result

This section aims at achieving the above objective.

Assumption 2: It is assumed that the system matrices A, B, H, K, L of NCSs are known.

This assumption is also widely adopted in previous studies.

The problem of completely stealthy attack sequence design is divided into the following two sub-problems: the design of the first attack vector and the design of subsequent attack vectors.

A. Stealthy Attack Sequence Design

Since the subsequence design completely relies on the first attack vector so as to achieve the residual on each step being zero, and the final attack effect analysis requires the entire attack sequence, the attack sequence construction principle is first investigated. The first attack vector is presumed as $\alpha_1 \neq \mathbf{0}$.

Theorem 1: The following attack sequence $\{\alpha_2, \alpha_3, \ldots\}$

$$\alpha_k = HA^{k-1}L\alpha_1, \ k \geq 2, \tag{11}$$

can achieve complete stealthiness, *i.e.,* $\Delta r_t = \mathbf{0}, \forall t \geq 2$.

Proof: Since the stealthiness performance is mainly related to the residual increment, by combining (7) and (8), the state equation of the variable increments can be obtained as follows

$$\begin{bmatrix} \Delta x_{k+1} \\ \Delta\hat{x}_{k+1} \\ \Delta r_{k+1} \end{bmatrix} = \begin{bmatrix} A & BK & \mathbf{O} \\ LHA & A+BK-LHA & \mathbf{O} \\ HA & -HA & \mathbf{O} \end{bmatrix} \begin{bmatrix} \Delta x_k \\ \Delta\hat{x}_k \\ \Delta r_k \end{bmatrix} + \begin{bmatrix} \mathbf{O} \\ L \\ I \end{bmatrix} \alpha_{k+1}$$
$$\triangleq \Gamma[\Delta x_k \ \Delta\hat{x}_k \ \Delta r_k]^T + [\mathbf{O} \ L \ I]^T\alpha_{k+1}. \tag{12}$$

It is noted that $[I - I \ \mathbf{O}]\Gamma = (A - LHA)[I - I \ \mathbf{O}]$, and then the residual increment Δr_k can be obtained as

$$\begin{aligned}
\Delta r_k &= [\mathbf{O} \ \mathbf{O} \ I][\Delta x_k \ \Delta\hat{x}_k \ \Delta r_k]^T \\
&= [\mathbf{O} \ \mathbf{O} \ I]\left\{\Gamma[\Delta x_{k-1} \ \Delta\hat{x}_{k-1} \ \Delta r_{k-1}]^T + [\mathbf{O} \ L \ I]^T\alpha_k\right\} \\
&= HA[I - I \ \mathbf{O}][\Delta x_{k-1} \ \Delta\hat{x}_{k-1} \ \Delta r_{k-1}]^T + \alpha_k \\
&= HA[I - I \ \mathbf{O}]\{\Gamma^{k-1}[\Delta x_0 \ \Delta\hat{x}_0 \ \Delta r_0]^T \\
&\quad + \sum_{i=1}^{k-1}\Gamma^{k-1-i}[\mathbf{O} \ L \ I]^T\alpha_i\} + \alpha_k \\
&= \alpha_k + HA\{(A - LHA)^{k-1}[I \ -I \ \mathbf{O}][\Delta x_0 \ \Delta\hat{x}_0 \ \Delta r_0]^T \\
&\quad + \sum_{i=1}^{k-1}(A - LHA)^{k-1-i}[I \ -I \ \mathbf{O}][\mathbf{O} \ L \ I]^T\alpha_i\} \\
&= \alpha_k + HA(A - LHA)^{k-1}(\Delta x_0 - \Delta\hat{x}_0) \\
&\quad + HA\sum_{i=1}^{k-1}(A - LHA)^{k-1-i}(-L)\alpha_i \\
&= \alpha_k - HA\sum_{i=1}^{k-1}(A - LHA)^{k-1-i}L\alpha_i.
\end{aligned} \tag{13}$$

Substituting attack sequence (11) into (13) leads to the residual performance under the designed attack,

$$\begin{aligned}
\Delta r_k &= HA^{k-1}L\alpha_1 - HA\sum_{i=2}^{k-1}(A - LHA)^{k-1-i}LHA^{i-1}L\alpha_1 \\
&\quad - HA(A - LHA)^{k-2}L\alpha_1 \\
&= HA\{A^{k-2} - \sum_{i=2}^{k-1}(A - LHA)^{k-1-i}LHA^{i-1} - (A - LHA)^{k-2}\}L\alpha_1 \\
&= HA\{A^{k-2} - \sum_{i=3}^{k-1}(A - LHA)^{k-1-i}LHA^{i-1} \\
&\quad - (A - LHA)^{k-3}LHA - (A - LHA)^{k-3}(A - LHA)\}L\alpha_1 \\
&= HA\{A^{k-2} + [-\sum_{i=3}^{k-1}(A - LHA)^{k-1-i}LHA^{i-2} - (A - LHA)^{k-3}]A\}L\alpha_1 \\
&\quad \cdots \\
&= HA\{A^{k-2} + [-\sum_{k-1}^{k-1}(A - LHA)^{k-1-i}LHA^{i-k+2} - (A - LHA)]A^{k-3}\}L\alpha_1 \\
&= HA\{A^{k-2} + [LHA - (A - LHA)]A^{k-3}\}L\alpha_1 \\
&= HA\{\mathbf{O}\}L\alpha_1 = \mathbf{0}, \quad k \geq 2.
\end{aligned} \tag{14}$$

Therefore, the residual increment is always zero from the second step. ■

From Theorem 1, the residual increment Δr_k can be always zero after the second step, which means that the residuals under the attack are the same as those without attack. This fact shows that the χ^2 detector, the SUM detector, and other similar residual based detectors cannot detect this strategy.

B. Selection of the First Attack

Section III-A ensures the complete stealthiness of subsequent attacks, however, there are still two key questions to be solved by the objective of this brief:

1) α_1 should satisfy the stealthiness requirement;

2) The entire attack strategy can cause sufficient damages.

It can be seen from Theorem 1 that α_1 determines the final attack influence. Therefore, the following choice of α_1 is given

$$\alpha_1 = \frac{\gamma}{\|HH^TL^TP\mathbf{e}_1\|}HH^TL^TP\mathbf{e}_1, \tag{15}$$

where $A^T = P\Lambda P^{-1}$, Λ is the Jordan normal form of A^T, $\Lambda = diag(\Lambda_1, \Lambda_2, \ldots, \Lambda_l)$, $l \leq n$,

$$\Lambda_i = \begin{pmatrix} \lambda_i & 1 & 0 & \cdots & 0 \\ 0 & \lambda_i & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda_i \end{pmatrix} \in \mathbb{R}^{r_i\times r_i}, \ \sum_{i=1}^{l} r_i = n,$$

$|\lambda_1| \geq |\lambda_2| \geq \cdots \geq |\lambda_l|$ and $P = [p_1 \ p_2 \ \cdots \ p_n]$, $p_1, p_2, \ldots, p_n \in \mathbb{R}^n$ are the eigenvalues and the generalized eigenvectors of matrix A^T, respectively.

Obviously, the attack vector defined by (15) satisfies the stealthiness requirement $\|\Delta r_1\| = \|\alpha_1\| \leq \gamma$.

Theorem 2: Attack sequence consisting of (11) and (15) is unbounded, *i.e.,* $\lim_{t\to\infty} \|\Delta e_t\| = \infty$.

Proof: By ignoring the residual, (12) can be simplified as

$$\begin{bmatrix} \Delta x_{k+1} \\ \Delta\hat{x}_{k+1} \end{bmatrix} = \begin{bmatrix} A & BK \\ LHA & A+BK-LHA \end{bmatrix} \begin{bmatrix} \Delta x_k \\ \Delta\hat{x}_k \end{bmatrix} + \begin{bmatrix} \mathbf{O} \\ L \end{bmatrix} \alpha_{k+1}. \tag{16}$$

From the contents of braces in (14) and by denoting $n = k-1$, it can be obtained that

$$A^{n-1} - \sum_{i=2}^{n}(A - LHA)^{n-i}LHA^{i-1} - (A - LHA)^{n-1} = \mathbf{O}. \quad (17)$$

By applying (11) and (15) into (16), and together with (17), it can be obtained that

$$\begin{aligned}\Delta e_k &= [I \ -I][\Delta x_k \ \Delta\hat{x}_k]^T \\ &= (A - LHA)[I \ -I][\Delta x_{k-1} \ \Delta\hat{x}_{k-1}]^T - L\alpha_k \\ &= (A - LHA)^k[I \ -I][\Delta x_0 \ \Delta\hat{x}_0]^T - \sum_{i=1}^{k}(A - LHA)^{k-i}L\alpha_i \\ &= -\sum_{i=2}^{k}(A - LHA)^{k-i}LHA^{i-1}L\alpha_1 - (A - LHA)^{k-1}L\alpha_1 \\ &= -A^{k-1}L\alpha_1, \quad k \geq 2. \end{aligned} \quad (18)$$

Therefore,

$$\begin{aligned}\lim_{k\to\infty}\Delta e_k &= \lim_{k\to\infty}A^{k-1}L\alpha_1 \\ &= \lim_{k\to\infty}(P^{-T}\Lambda^T P^T)^{k-1}LHH^TL^TP\mathbf{e}_1\gamma/\|HH^TL^TP\mathbf{e}_1\|. \end{aligned} \quad (19)$$

Denoted $P^TLHH^TL^TP\mathbf{e}_1 \triangleq \mathbf{s} = [s_1 \ s_2 \ \cdots \ s_n]^T \in \mathbb{R}^n$, then $s_1 = \mathbf{e}_1^TP^TLHH^TL^TP\mathbf{e}_1$.

Suppose $s_1 = 0$, namely $H^TL^TP\mathbf{e}_1 = H^TL^Tp_1 = \mathbf{0}$. It is noted that $A^Tp_1 = \lambda_1 p_1$, then

$$p_1^T(A - LHA) = \lambda_1 p_1^T - (H^TL^Tp_1)^TA = \lambda_1 p_1^T, \quad (20)$$

which contradicts the fact that $\rho(A - LHA) < 1$. Therefore, $s_1 \neq 0$. Then, the following equalities hold as long as $s_1 \neq 0$,

$$\begin{aligned}\lim_{k\to\infty}\mathbf{e}_{r_1}^T(\Lambda^T)^{k-1}\mathbf{s} &= \lim_{k\to\infty}\sum_{i=1}^{r_1}\binom{k-1}{r_1-i}\lambda_1^{k-1-r_1+i}s_i \\ &= \mathcal{O}(\lim_{k\to\infty}\binom{k-1}{r_1-1}\lambda_1^{k-r_1}s_1) = \infty. \end{aligned} \quad (21)$$

Since λ_1 is the eigenvalue with the maximum modulus and P is invertible, it can be derived that

$$\begin{aligned}&\|\lim_{k\to\infty}(P^{-T}\Lambda^TP^T)^{k-1}LHH^TL^TP\mathbf{e}_1\| \\ &= \lim_{k\to\infty}\|P^{-T}(\Lambda^T)^{k-1}P^T\mathbf{s}\| = \infty, \end{aligned} \quad (22)$$

and finally, $\lim_{k\to\infty}\|\Delta e_k\| = \infty$, $\lim_{k\to\infty}\|e_k^a\| = \infty$. Therefore, the proposed attack strategy is unbounded. ■

From Theorem 2, the attack strategy defined by (11) and (15) can satisfy the unbounded attack requirement, and together with satisfying the completely stealthiness requirement, the proposed attack strategy achieves the brief's objective.

C. Stealthiness Performance for Static Detection Methods

Another question is whether this attack strategy can bypass the widely used static detection methods. Since the most commonly used static method is the WLS method whose detection principle is consistent with other static methods, this section verifies the stealthiness of the proposed attack strategy by testing whether it can bypass the WLS detector.

Theorem 3: Subsequent attack sequence (11) can achieve complete stealthiness for the static WLS detector, *i.e.,* $\Delta r_t^s = \mathbf{0}$, $\forall t \geq 1$.

Proof: By applying (15) into (4), the residual increment of the WLS detector at the first step can be derived that

$$\begin{aligned}\Delta r_1^s &= [I - H(H^TRH)^{-1}H^TR]\alpha_1 \\ &= [I - H(H^TRH)^{-1}H^TR]HH^TL^TP\mathbf{e}_1\gamma/\|HH^TL^TP\mathbf{e}_1\| \\ &= \{HH^TL^TP\mathbf{e}_1 - H[(H^TRH)^{-1}(H^TRH)]H^TL^TP\mathbf{e}_1\} \\ &\quad \times\gamma/\|HH^TL^TP\mathbf{e}_1\| \\ &= \{HH^TL^TP\mathbf{e}_1 - HH^TL^TP\mathbf{e}_1\}\gamma/\|HH^TL^TP\mathbf{e}_1\| = \mathbf{0}. \end{aligned}$$

Therefore, the first attack vector can bypass the WLS detector.

Applying (11) into (4) leads to the following results

$$\begin{aligned}\Delta r_k^s &= [I - H(H^TRH)^{-1}H^TR]\alpha_k \\ &= (H - H(H^TRH)^{-1}H^TRH)A^{k-1}L\alpha_1 \\ &= (\mathbf{0})A^{k-1}L\alpha_1 = \mathbf{0}. \end{aligned}$$

Therefore, other attack vectors bypass the WLS detector. ■

From Theorem 3, it is proved that the proposed attack strategy also achieves the desired stealthiness performance under the surveillance of static estimation.

IV. Numerical Simulation

This section verifies whether the proposed attack strategy can achieve the objectives of complete stealthiness and unbounded attack.

The numerical simulation is carried out on the IEEE 6-bus power system, which is also used for the verification of the FDI attack with "complete stealthiness" in [21]. The main system model and its parameters are the same as those in [21]. The generator rotor angle and rotation rate are sampled separately.

Four sets of simulations are performed: the case without attack and the cases under the following three attacks.

Attack I satisfying Definition 2 is designed according to [17] and is given as follows

$$\alpha_1^I = \alpha^\dagger, \quad \alpha_k^I = 0.9811 \times \sum_{i=2}^{k}\lambda^i\alpha^*, \ k \geq 2,$$

where $\alpha^* = [0.3932 \ -1.2454 \ 0.0672]^T$, $\lambda = 1.0417$, $\alpha^\dagger = [0.4019 \ -1.2728 \ 0.0687]^T$.

Attack II satisfying Definition 3 is designed according to [21],

$$\alpha_1^{II} = \alpha^\dagger,$$

$$\alpha_k^{II} = \begin{cases} 0.9811 \times \sum_{i=2}^{k}\lambda^i\alpha^*, & 2 \leq k \leq 5, \\ (0.9811 \times \sum_{i=2}^{5}\lambda^i + 0.1822 \times \sum_{i=6}^{k}\lambda^i)\alpha^*, & k > 5, \end{cases}$$

where α^*, λ and $\alpha^\dagger$ are defined as those in **Attack I**.

Attack III satisfying Definition 4 is designed according to the attack strategy proposed in this brief,

$$\alpha_1^{III} = [-0.0062 \ -0.0063 \ 1.3264]^T, \ \alpha_k^{III} = HA^{k-1}\alpha_1^{III}, \ k \geq 2.$$

In the simulations, the state deviations and the detection results of three detectors (χ^2 detector, SUM detector and WLS detector) are investigated and shown in Fig. 1. The detection thresholds are set to be 12.84 and 4.85 according to the definitions of the detectors.

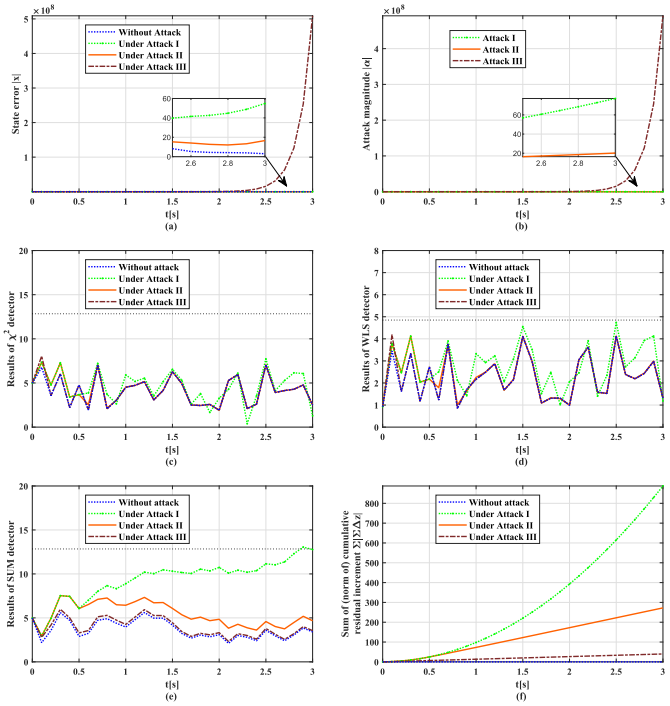

Fig. 1. The proposed FDI attack strategy achieves a better performance in damage and stealthiness: (a) Attack III causes far more state deviations; (b) Attack magnitudes increase exponentially; (c) All attacks bypass the χ^2 detector; (d) All attacks bypass the WLS detector; (e) Attacks II and III bypass the SUM detector; (f) Attack III causes less cumulative residual increments.

From Figs. 1 (a) and (b), Attack III has more magnitudes and causes far more deviations (508935027) than other attacks (Attack I: 51.8422, Attack II: 13.5746), and the attack effect increased by $508935027/51.8422-1=9817001$ times. From Figs. 1 (c) and (d), the χ^2 and WLS detectors cannot prevent these advanced and well-crafted attacks. From Fig. 1 (e), the performance of Attack III is closer to that in the unattacked case than Attack II under the surveillance of the SUM detector, the increments of detection indicator caused by Attack I, Attack II, and Attack III are 9.3666, 1.2694, and 0.1501 ($1-0.1501/1.2694=88.17\%$ reduction), respectively. From Fig. 1 (f), Attack III causes much less sum of cumulative residual increments (39.7940) than other attacks (Attack I: 887.5300, Attack II: 272.3680). This is a reduction of ($1-39.7940/272.3680=85.39\%<88.17\%$), which shows the expected stealthiness of the proposed method.

Remark 1: Since the proposed attack strategy causes 85.39% less sum of cumulative residual increments compared with the existing attacks, the exposure risk of this attack in the presence of the SUM detector is reduced by no less than 85.39%. At the same time, compared with other attacks, this attack quickly causes a large number of state deviations in a short period of time, which means that it causes huge damage to the NCS.

V. Conclusion

This brief proposes an FDI attack strategy with the desired stealthiness performance against estimation in terms of χ^2 detector and SUM detector in networked control systems. This attack strategy is theoretically capable of making the residuals almost everywhere unchanged and ultimately causing infinite state deviations. In the simulation of IEEE 6-bus systems, compared with other existing attack strategies, this method reduces the sum of cumulative residual increments by 85.39% and results in a 981700188% increase in the state deviation, which shows that the proposed attack strategy has better performance in both stealthiness and attack effect.

References

[1] X. Zhang et al., "Networked control systems: A survey of trends and techniques," *IEEE/CAA J. Automatica Sinica*, vol. 7, no. 1, pp. 1–17, Jan. 2020.

[2] T. Alpcan and S. Buchegger, "Security games for vehicular networks," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 280–290, Feb. 2011.

[3] R. Dong et al., "Study on remote control system of rural water treatment equipment based on labview," in *Proc. Int. Conf. Robots Intell. Syst. (ICRIS)*, Changsha, China, 2018, pp. 44–47.

[4] X. Dong et al., "Power flow analysis considering automatic generation control for multi-area interconnection power networks," *IEEE Trans. Ind. Appl.*, vol. 53, no. 6, pp. 5200–5208, Nov./Dec. 2017.

[5] F. Farivar, M. S. Haghighi, A. Jolfaei, and S. Wen, "On the security of networked control systems in smart vehicle and its adaptive cruise control," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 6, pp. 3824–3831, Jun. 2021.

[6] J. Zhou, J. Shang, Y. Li, and T. Chen, "Optimal DoS attack against LQR control channels," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 68, no. 4, pp. 1348–1352, Apr. 2021.

[7] K.-D. Lu and Z.-G. Wu, "Multi-objective false data injection attacks of cyber-physical power systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 9, pp. 3924–3928, Sep. 2022, doi: 10.1109/TCSII.2022.3181827.

[8] Z.-H. Pang, L.-Z. Fan, Z. Dong, Q.-L. Han, and G.-P. Liu, "False data injection attacks against partial sensor measurements of networked control systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 69, no. 1, pp. 149–153, Jan. 2022.

[9] L. Gao, B. Chen, and L. Yu, "Fusion-based FDI attack detection in cyber-physical systems," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 67, no. 8, pp. 1487–1491, Aug. 2020.

[10] L. Che, X. Liu, T. Ding, and Z. Li, "Revealing impacts of cyber attacks on power grids vulnerability to cascading failures," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 66, no. 6, pp. 1058–1062, Jun. 2019.

[11] J. Duan, W. Zeng, and M. Y. Chow, "Resilient distributed DC optimal power flow against data integrity attack," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3543–3552, Jul. 2018.

[12] I. Lukicheva, D. Pozo, and A. Kulikov, "Cyberattack detection in intelligent grids using non-linear filtering," in *Proc. IEEE PES Innov. Smart Grid Technol. Europe*, 2018, pp. 1–6.

[13] M. G. Kallitsis, S. Bhattacharya, S. Stoev, and G. Michailidis, "Adaptive statistical detection of false data injection attacks in smart grids," in *Proc. IEEE Global Conf. Signal Inf. Process.*, 2016, pp. 826–830.

[14] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Security*, vol. 14, no. 1, p. 13, 2011.

[15] B. Liu and H. Ye, "Statistical χ^2 testing based fault detection for linear discrete time-delay systems," *Acta Automatica Sinica*, vol. 40, no. 7, pp. 1278–1284, 2014.

[16] C.-Z. Bai, F. Pasqualetti, and V. Gupta, "Security in stochastic control systems: Fundamental limitations and performance bounds," in *Proc. Amer. Control Conf.*, 2015, pp. 195–200.

[17] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," in *Proc. 1st Workshop Secure Control Syst.*, Stockholm, Sweden, 2010, pp. 1–6.

[18] L. Hu, Z. Wang, Q. Han, and X. Liu, "State estimation under false data injection attacks: Security analysis and system protection," *Automatica*, vol. 87, pp. 176–183, Jan. 2018.

[19] G.-Y. Yang and X.-J. Li, "Complete stealthiness false data injection attacks against dynamic state estimation in cyber-physical systems," *Inf. Sci.*, vol. 586, pp. 408–423, Mar. 2022.

[20] D. Ye and T. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2338–2345, Jun. 2020.

[21] D. Ye and T. Zhang, "False data injection attacks with complete stealthiness in cyber-physical systems: A self-generated approach," *Automatica*, vol. 120, pp. 109–117, Oct. 2020.

[22] Y. Liu and L. Cheng, "Relentless false data injection attacks against Kalman filter based detection in smart grid," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 3, pp. 1238–1250, Sep. 2022.