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

False Data Injection Attack for Switched Systems

Rui Zhao, Zhiqiang Zuo, Yijing Wang, and Wentao Zhang

Abstract— **This paper studies the secure state estimation problem for switched systems. The single/joint false data injection attacks are designed with the aim at altering the sensor signal and/or switching signal. Firstly, it is shown that the attack will steer system state to infinity but could be detectable by χ^2 detector when only the switching signal is attacked. In addition, the attack acting on sensor signal is designed, which can be recognized by the summation (SUM) detector but fails by χ^2 detector. Then a joint attack strategy is devised and a sufficient condition is given to guarantee that the joint attack is strictly stealthy. The joint attack performs well since it can launch a strictly stealthy attack compared with the sensor signal attack. Finally, a numerical example is given to verify the theoretical results.**

Index Terms— **False data injection attack, switched system, joint attack, stealthy attack**

I. Introduction

With the development of network and compute technology, network control systems have attracted more and more attention. One of the accompanying problem is security, which is an interesting issue and has become a major topic in the past few decades [1], [2]. There are many cyber risks and threats in practical applications, such as power grids [3], intelligent transportation system [4], etc. Moreover, the cyber security issue will also lead to physical problems even economic losses, for instance, the nuclear facility in Iran [5] and the Ukraine power grid attack [6].

Generally, there are two types of attacks [7]: denial-of-service (DoS) attack and deception attack. The former deteriorates system performance by blocking information transmission, which damages the real-time performance of information [8], [9]. The latter brings negative effects on system dynamics or even make system unstable by modifying the transmitted signal or injecting false data to compromise the accuracy of information [10]. Nowadays, χ^2 detector and summation (SUM) detector are commonly used for control systems which are based on estimation residual. More recently, massive research interests focus on the undetectable deception attack, which undermines the stability of the system while bypassing the detector [11], [12].

This work was supported by the National Natural Science Foundation of China (grants 62173243 and 61933014) and the Foundation (No. Scip202107) of Key Laboratory of System Control and Information Processing, Ministry of Education, Shanghai, 200240.

R. Zhao, Z. Zuo and Y. Wang are with the Tianjin Key Laboratory of Intelligent Unmanned Swarm Technology and System, School of Electrical and Information Engineering, Tianjin University, Tianjin 300072, China. W. Zhang was with the School of Electrical and Information Engineering, Tianjin University, Tianjin, 300072, P. R. China, and is currently with the School of Electrical and Electronic Engineering, Nanyang Technological University, Singapore 639798. (e-mail: ruizhao@tju.edu.cn; zqzuo@tju.edu.cn; yjwang@tju.edu.cn; wentao.zhang@ntu.edu.sg)

For non-switched systems, some progress has been made in the literature. [13] was a pioneering work studying stealthy false date injection attack, and a necessary and sufficient condition was given. Inspired by this, a completely stealthy attack using a self-generated approach was proposed in [14]. The constrained sensor attack in which part of sensor channels are compromised was investigated in [15]. Ref. [16] designed a reset attack that enables to diverge the states or steer them to a target set. Moreover, much effort has been paid on studying the effect of joint attack, e.g., injecting false date into sensor and estimator [17], sensor and controller [18], [19]. Notice that the above results require the accurate model of the considered system. Recently, Ref. [20] proposed an attack design method without the knowledge of the gain of estimator.

Switched system is a useful tool to describe practical systems such as hot strip mill [21], networked stirred tank reactors [22], power systems [23] and so on. It is usually composed of a class of subsystems and a logic rule managing how these subsystems operate [24]. Unfortunately, the existing methods for stealthy attack are generally not suitable for switched system, since they can only deal with a time-invariant system. It is well known that the stabilization of switched system not only depends on the dynamics of subsystems, but also is closely related to the switching signal [25]. Furthermore, the asynchronous behavior between controller mode and subsystem will degrade the system performance [26].

It is noted that few work has been done for cyber security of switched systems. Ref. [27] investigated the resilient control for switched system under switching attack, while the data injection attack was not involved. In [28], state-feedback switched system suffering from signal and switching attacks was discussed. A generalization focusing on switching attack was reported in [29], where both unknown input and nonlinear dynamics were taken into account. A downside uncovered in the existing literature is that they do not account for the attack of destroying the system without triggering the alarm.

Motivated by the above discussions on data injection attack and the feature of switched system, we aim to investigate the attack design issue for switched system. Different from non-switched systems, the switching signal is essential. By taking the switching signal into full consideration, the single and joint attacks are designed. Furthermore, the capability of bypassing the residual-based detector is discussed in detail. It should be noted that the latter has not been studied in the existing literature for switched system suffering from attack. And the comparison results of all generic attacks are

given. More specifically, the contributions of this paper can be summarized as follows:

1) A switching signal is designed to steer the state to infinity which is easy to implement in practice without the knowledge of system matrices. Nevertheless, it is detected by traditional χ^2 detector and SUM detector.
2) A sensor signal attack is devised to be undetectable for χ^2 detector with the knowledge of system mode. However, it fails for SUM detector.
3) A criterion for strict stealthiness is derived for joint attack on switching signal and sensor signal, which makes sure that there is no alarm from the detector based on the estimation residual.

The remainder of this paper is organized as follows. Section II gives some preliminaries and system specification. The sensor and/or switching signal attacks for switched systems are presented in Section III. Section IV gives a numerical example to verify the obtained results. Finally, we conclude this paper in Section V.

II. Problem Formulation

Consider a switched system with disturbance described by

$$x(k+1) = A_{\sigma(k)}x(k) + B_{\sigma(k)}u(k) + w(k) \quad (1)$$
$$y(k) = C_{\sigma(k)}x(k) + v(k) \quad (2)$$

where $x(k) \in \mathbb{R}^{n_x}$, $u(k) \in \mathbb{R}^{n_u}$ and $y \in \mathbb{R}^{n_y}$ are system state, control input and measurement output. $w(k) \in \mathbb{R}^{n_x}$ and $v(k) \in \mathbb{R}^{n_y}$ are process noise and sensor noise obeying identically Gaussian distribution, i.e., $w(k) \sim N(0, \mathcal{W})$ and $v(k) \sim N(0, \mathcal{V})$. $\sigma(k) \in \mathcal{M} \triangleq \{1, 2, \cdots, m\}$ is the switching signal in which m is the number of subsystems. A_i, B_i and C_i $(i \in \mathcal{M})$ are constant matrices with appropriate dimensions.

In this paper, the system state is not available, then an estimator is designed as

$$\hat{x}(k+1) = A_{\hat{\sigma}(k)}\hat{x}(k) + B_{\hat{\sigma}(k)}u(k) + L_{\hat{\sigma}(k)}z(k+1)$$

with estimator residual being

$$z(k+1) = y(k+1) - C_{\hat{\sigma}(k)}(A_{\hat{\sigma}(k)}\hat{x}(k) + B_{\hat{\sigma}(k)}u(k))$$

where $\hat{\sigma}(k) \in \mathcal{M}$ is the mode of the estimator. For normal switched system, $\hat{\sigma}(k) = \sigma(k)$. In terms of the value of estimation, the feedback control signal is $u(k) = K_{\hat{\sigma}(k)}\hat{x}(k)$ where $K_{\hat{\sigma}(k)}$ is the controller gain. Without loss of generality, we assume that each pair (A_p, B_p) is stabilizable which means that we can always find an appropriate controller gain K_p such that $A_p + B_pK_p$ is Schur stable for all $p \in \mathcal{M}$.

Fig. 1 exhibits the system structure and potential security risks. The sensor signal and switching signal are transmitted via network, which are vulnerable. The attacker can inject false data into sensor-to-controller channel using sensor signal attack data $a_y(k)$ and attacked switching signal (it is also the controller mode) $\sigma^a(k)$. The blue diagrams represent the actual system mode $\sigma(k)$, while the vanilla diagrams, including the color of estimator, indicate the attacked switching signal $\sigma^a(k)$. The detector works according to the estimator

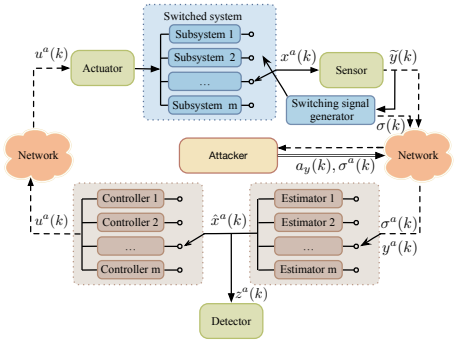

Fig. 1. The switched system structure under cyber attack

residual, for example, χ^2 detector or SUM detector [15], [30].

In the following analysis, the impact of sensor signal attack and/or switching signal attack on the system will be investigated. When the false data is injected into the sensor signal, the attacked sensor signal (it is also the input of estimator) becomes $y^a(k) = \widetilde{y}(k) + a_y(k)$ with $\widetilde{y}(k)$ being the output for switched system suffering from attack. Moreover, the switching signal may be changed due to the attack. As a result, one has $\hat{\sigma}(k) = \sigma^a(k)$. Here we consider the scenario where the attacker has the knowledge of all subsystem matrices, i.e., A_p, B_p, C_p, K_p and $L_p (p \in \mathcal{M})$.

The system dynamics suffering from attack now turns to be

$$\begin{aligned}
x^a(k+1) =& A_{\sigma(k)}x^a(k) + B_{\sigma(k)}u^a(k) + w(k)\\
\widetilde{y}(k) =& C_{\sigma(k)}x^a(k) + v(k)\\
\hat{x}^a(k+1) =& A_{\sigma^a(k)}\hat{x}^a(k) + B_{\sigma^a(k)}u^a(k) + L_{\sigma^a(k)}z^a(k+1)\\
z^a(k+1) =& y^a(k+1) - C_{\sigma^a(k)}(A_{\sigma^a(k)}\hat{x}(k) + B_{\sigma^a(k)}u^a(k)).
\end{aligned}$$

Define the estimator error without/with attack be $e(k) = x(k) - \hat{x}(k)$ and $e^a(k) = x^a(k) - \hat{x}^a(k)$. Then the estimator error difference $\Delta e(k) = e^a(k) - e(k)$ and estimator residual difference $\Delta z(k) = z^a(k) - z(k)$ admit

$$\begin{aligned}
\Delta e(k+1) =& A_p\Delta e(k) + L_p\Delta z(k+1) \quad (3)\\
&+ (B_p - B_q)u^a(k) - (A_q - A_p)\hat{x}^a(k)\\
&- (L_q - L_p)z^a(k+1)\\
\Delta z(k+1) =& C_pA_p\Delta e(k) + (C_pB_p - C_qB_q)u^a(k) \quad (4)\\
&+ (C_pA_p - C_qA_q)\hat{x}^a(k) + a_y(k+1)
\end{aligned}$$

where $p \in \mathcal{M}$ and $q \in \mathcal{M}$ represent the system mode $\sigma(k)$ and controller mode $\sigma^a(k)$, respectively.

In this paper, a detector is designed according to the estimator residual, for example, χ^2 detector and SUM detector. For χ^2 detector, its mathematical expression is $G(k) = z^T(k)(C_{\sigma(k)}\Gamma C_{\sigma(k)}^T + R)^{-1}z(k)$ where Γ is the steady estimation error covariance and R is the variance of measurement noise $v(k)$. If $G(k) > \alpha$, then an alarm will be triggered. SUM detector [30] has the form $J(k) = \frac{1}{k}(\sum_{i=0}^{k} z(k))^T(C_{\sigma(k)}\Gamma C_{\sigma(k)}^T + R)^{-1}\sum_{i=0}^{k} z(k)$. If $J(k) > \beta$, then an alarm will be triggered and the attack is revealed. It is noted that the attack can be detected by SUM detector

even if the attack is stealthy for χ^2 detector, see [14], [30] for details.

Definition 1 ([13], [18]): For a given attack sequence $\{a_y(k), \sigma^a(k)\}$, if $\lim_{k\to\infty} \|\Delta e(k)\| = \infty$ and $\|\Delta z(k)\| \leq M$ hold where M is a small positive constant, then it is said to be stealthy. Moreover, if $M = 0$, the attack is strictly stealthy.

Remark 1: The definition of stealthy attack was originally proposed in [13], and it is shown that such an attack makes system diverge without alarming χ^2 detector. Nevertheless, the attack may be detected by SUM detector as stated in [14], [30]. Then the concept of strictly stealthy attack was given in Ref. [18], whose condition is strong than two expressions in [14], i.e., complete stealthiness and energy stealthiness. The strict stealthiness defined here requires that the residual is equal to zero at any time. However, Ref. [14] just needs $\lim_{k\to\infty} \|\Delta z(k)\| = 0$. It is obvious that the attack sequence that meets the conditions of this paper is also valid for [14]. Naturally, a strictly stealthy attack cannot be detected by χ^2 detector and SUM detector since it is no longer detectable.

In this paper, we aim to design an attack mechanism on sensor-to-controller channel for switched system so that the attack cannot be detected by residual-based detector.

III. Main results

A. Switching Signal Attack

In this subsection, we consider the case where the attack only acts on the switching signal, i.e., $a_y(k) = 0$ and $\sigma^a(k) \neq \sigma(k)$. The existing literature points out that asynchronous behavior in which the controller mode differs from the subsystem mode will degrade system performance, see [26], [31]. When the switching signal received by the estimator is amended by the attacker, not only the controller mode is different from the system mode, but also the state estimation error $e(k)$ may be greater than the normal one. In this case, the estimation error under switching signal attack becomes

$$\begin{aligned} & e^a(k+1) \\ = \; & (A_p - L_q C_p A_p) e^a(k) - L_q C_p w(k) \\ & + (B_p - B_q - L_q C_p B_p + L_q C_q B_q) K_q \hat{x}^a(k) \\ & + ((A_p - L_q C_p A_p) - (A_q - L_q C_q A_q)) \hat{x}^a(k) \\ = \; & \begin{bmatrix} A_p - L_q C_p A_p & \Xi_{pq}^{12} \end{bmatrix} \begin{bmatrix} e^a(k) \\ \hat{x}^a(k) \end{bmatrix} - L_q C_p w(k) \end{aligned}$$

where $\Xi_{pq}^{12} = (I - L_q C_p)(A_p + B_p K_q) - (I - L_q C_q)(A_q + B_q K_q)$. p and q correspond to switched system mode $\sigma(k)$ and attacked switching signal $\sigma^a(k)$, respectively.

Define $\psi(k) = \begin{bmatrix} e^a(k) \\ \hat{x}^a(k) \end{bmatrix}$, we have

$$\begin{aligned} & \psi(k+1) \\ = \; & \begin{bmatrix} A_p - L_q C_p A_p & \Xi_{pq}^{12} \\ L_q C_p A_p & \Xi_{pq}^{22} \end{bmatrix} \psi(k) - \begin{bmatrix} L_q C_p \\ L_q C_p \end{bmatrix} w(k) \\ = \; & \mathcal{A}_{pq} \psi(k) - \mathcal{E}_{pq} w(k) \end{aligned} \tag{5}$$

where $\Xi_{pq}^{22} = (I - L_q C_q)(A_q + B_q K_q) + L_q C_p (A_p + B_p K_q)$.

Proposition 1: For switching signal sequence $\Sigma(k) \triangleq \{\sigma(1), \cdots, \sigma(k)\}$ and attacked switching signal sequence $\Sigma^a \triangleq \{\sigma^a(1), \cdots, \sigma^a(k)\}$, if $\| \prod_{i=0}^{k} \mathcal{A}_{\sigma(i)\sigma^a(i)} \| > 1$, then switched system (1) under solely switching signal attack is unstable.

Proof: From (5), one has

$$\begin{aligned} & \psi(k+1) \\ = \; & \mathcal{A}_{\sigma(k)\sigma^a(k)} \psi(k) - \mathcal{E}_{\sigma(k)\sigma^a(k)} w(k) \\ = \; & \mathcal{A}_{\sigma(k)\sigma^a(k)} \mathcal{A}_{\sigma(k-1)\sigma^a(k-1)} \psi(k-1) \\ & - \mathcal{A}_{\sigma(k)\sigma^a(k)} \mathcal{E}_{\sigma(k-1)\sigma^a(k-1)} w(k-1) - \mathcal{E}_{\sigma(k)\sigma^a(k)} w(k) \\ = \; & \cdots \\ = \; & \prod_{i=0}^{k} \mathcal{A}_{\sigma(i)\sigma^a(i)} \psi(0) - \sum_{j=0}^{k-1} \Big(\prod_{i=j+1}^{k} \mathcal{A}_{\sigma(i)\sigma^a(i)} \Big) \mathcal{E}_{\sigma(j)\sigma^a(j)} w(j) \\ & - \mathcal{E}_{\sigma(k)\sigma^a(k)} w(k) \end{aligned}$$

where $\Theta(k) = -\sum_{j=0}^{k-1} (\prod_{i=j+1}^{k} \mathcal{A}_{\sigma(i)\sigma^a(i)}) \mathcal{E}_{\sigma(j)\sigma^a(j)} w(j) - \mathcal{E}_{\sigma(k)\sigma^a(k)} w(k)$. If $\| \prod_{i=0}^{k} \mathcal{A}_{\sigma(i)\sigma^a(i)} \| > 1$, it yields

$$\begin{aligned} \|\psi(k+1)\| \geq \; & \Big\| \prod_{i=0}^{k} \mathcal{A}_{\sigma(i)\sigma^a(i)} \Big\| \|\psi(0)\| - \|\Theta(k)\| \\ > \; & \|\psi(0)\| - \|\Theta(k)\|. \end{aligned}$$

Let us consider a specific case where the system is free of noise, i.e., $w(k) = 0$. Then we have $\|\psi(k+1)\| > \|\psi(0)\|$. Obviously, the system will diverge. ■

Remark 2: In Proposition 1, a sufficient condition is derived using inequality scaling method, which brings some conservatism. Moreover, from perspective of the attacker, the worst case is that the system is free of noise. Proposition 1 implies that the attacked switching signal $\sigma^a(k)$ can be chosen to make $\lambda_{\max}(\mathcal{A}_{\sigma(k)\sigma^a(k)}) > 1$. On the other hand, it means that the vulnerability of switched system is related to the controller gain K_p and estimator gain L_p for all $p \in \mathcal{M}$. Therefore, well-designed gains can enhance the cyber security. Furthermore, a longer operating time of secured subsystem in designing switching law is expected to get preferable level of security.

Note that the estimator residual under attack is

$$\begin{aligned} & z^a(k+1) \\ = \; & C_p(A_p x^a(k) + B_p u(k) + w(k)) - C_q(A_q \hat{x}^a(k) + B_q u(k)) \\ = \; & \begin{bmatrix} C_p A_p & C_p(A_p + B_p K_q) - C_q(A_q + B_q K_q) \end{bmatrix} \psi(k) \\ = \; & \mathcal{C}_{pq} \psi(k). \end{aligned}$$

When $\psi(k)$ approaches to infinity, there exists an instant k such that $\|z^a(k)\| > 2M$ due to the fact $rank(\mathcal{C}_{pq}) > 0$. Note that the estimator residual of system without attack is less than M, namely, $\|z(k)\| \leq M$. This further derives $\|\Delta z(k)\| \geq \|z^a(k)\| - \|z(k)\| > M$, which implies that the attack is detectable by χ^2 detector, let alone SUM detector.

B. Sensor Signal Attack

In Subsection III-A, the attack only acts on the switching signal. In what follows, we will discuss whether there exists

a sensor signal attack that could bypass the traditional χ^2 detector, that is, the residual difference is less than a smaller positive constant M. More specifically, we consider the case $a_y(k) \neq 0$ and $\sigma(k) = \sigma^a(k)$. Then (3) and (4) become

$$\begin{aligned} \Delta e(k+1) = &\ A_p \Delta e(k) + L_p \Delta z(k+1) \quad (6) \\ \Delta z(k+1) = &\ C_p A_p \Delta e(k) + a_y(k+1) \quad (7) \end{aligned}$$

where $p = \sigma(k) \in \mathcal{M}$. Inspired by [15], the attack signal can be designed as

$$a_y(k+1) = -C_{\sigma(k)} A_{\sigma(k)} \Delta e(k) + \eta M I^t_{n_y} \quad (8)$$

with $\eta \in (0,1)$ and $I^t_{n_y} = [\overbrace{0, \ldots, 0}^{t-1}, 1, 0, \ldots, 0]^T_{n_y}$. Substituting (8) into (7), we have $\Delta z(k+1) = \eta M I^t_{n_y}$. It is obvious that $\|\Delta z(k)\| \leq M$, which means that the attack cannot be detected.

Proposition 2: There exists no solely sensor signal attack with strict stealthiness for switched system (1).

Proof: To launch strictly stealthy attack, it requires that $\|\Delta z(k)\| = 0$ from Definition 1. Since the initial conditions are $x(0) = x^a(0)$ and $\hat{x}(0) = \hat{x}^a(0)$, one has $\Delta e(0) = 0$. The attack will not affect system (6) as $\Delta e(k) = 0$ for all $k \geq k_0$. Hence, we cannot get $\lim_{k\to\infty} \|\Delta e(k)\| \to \infty$ and $\Delta z(k) = 0$, which implies that the strictly stealthy attack will not be launched. ∎

Proposition 2 suggests that the sensor signal attack for switched system (1) can be detected by SUM detector. More specifically, we have $\sum_{i=0}^{k} \Delta z(k) = k * \eta M I^t_{n_y}$ since $\Delta z(k+1) = \eta M I^t_{n_y}$. Considering the definition of $J(k)$, it is clear that $J(k) \to \infty$ as $k \to \infty$. Thus the attack indeed is detected by SUM detector.

C. Joint attack on switching signal and sensor signal

In Subsection III-B, the sensor signal attack is detectable for SUM detector since the estimator residual always exists even if it is small. As pointed out in [17]–[19], the joint attack has a greater possibility to launch a more cunning attack. By taking the special feature of switched systems into account, we address the joint attack strategy acting on both switching signal and sensor signal. In the sequel, we focus on how to design a joint attack to bypass the traditional χ^2 detector and SUM detector. When the attacked switching signal sequence is $\Sigma^a(k) = \{\sigma^a(1), \cdots, \sigma^a(k)\}$, the attack signal on output sequence becomes $\mathbb{A}(k) = \{a_y(1), \cdots, a_y(k)\}$ where

$$\begin{aligned} a_y(k+1) = &\ -C_p A_p \Delta e(k) + (C_q A_q - C_p A_p)\hat{x}^a(k) \\ &- (C_p B_p - C_q B_q) K_q \hat{x}^a(k) \end{aligned} \quad (9)$$

with $p, q \in \mathcal{M}$ representing $\sigma(k)$ and $\sigma^a(k)$ for brevity. For attacker, $\Delta e(k)$ can be calculated by (3) and the estimation state under attack $\hat{x}^a(k)$ can be eavesdropped.

Theorem 1: For attacked switching signal sequence $\Sigma^a(k) \triangleq \{\sigma^a(1), \cdots, \sigma^a(k)\}$, if the attack signal acting on the sensor satisfies (9) and $\rho(A_p) > 1$ for all $p \in \mathcal{M}$, then this joint attack is strictly stealthy.

Proof: Substituting (9) into (4), it is straightforward to get $\|\Delta z(k)\| = 0$. This means that the attack cannot be detected by the residual-based detector. Moreover, it suggests that $z(k) = z^a(k)$. Therefore, (3) turns to be

$$\begin{aligned} \Delta e(k+1) = &\ A_p \Delta e(k) + (L_p - L_q) z(k+1) \\ &+ (A_p + B_p K_q - A_q - B_q K_q)\hat{x}^a(k). \end{aligned}$$

Let $\zeta(k) = \begin{bmatrix} \Delta e(k) \\ \hat{x}^a(k) \end{bmatrix}$, then we have

$$\begin{aligned} &\zeta(k+1) \quad (10) \\ = &\begin{bmatrix} A_p & \widetilde{A}_{pq} - \overline{A}_q \\ 0 & \overline{A}_q \end{bmatrix} \zeta(k) + \begin{bmatrix} L_p - L_q \\ L_q \end{bmatrix} z(k+1) \\ = &\ \Omega_{pq} \zeta(k) + \mathcal{L}_{pq} z(k+1) \end{aligned}$$

where $\widetilde{A}_{pq} = A_p + B_p K_q$ and $\overline{A}_q = A_q + B_q K_q$. Since the origin switched system without attack is stable, then $\|z(k)\| = \|C_p A_p e(k)\|$ is bounded.

Considering the dynamics of the estimator, one has

$$\begin{aligned} &\|\hat{x}^a(k)\| \\ \leq &\ \|\prod_{i=0}^{k} \overline{A}_{\sigma^a(i)}\| \|\hat{x}^a(0)\| + \|\sum_{j=0}^{k-1} \prod_{i=j+1}^{k} \overline{A}_{\sigma^a(i)} L_{\sigma^a(j)} z(j)\|. \end{aligned}$$

Since $\overline{A}_p (p \in \mathcal{M})$ is Schur stable, $\hat{x}^a(k)$ will not diverge.

Note that (10) gives $\|\zeta(k+1)\| \to \infty$ as time goes to infinity since $\|\Omega_{pq}\| > 1$ when $\rho(A_p) > 1$. Due to the fact that $\hat{x}^a(k)$ has an upper bound, it is obvious that $\|\Delta e(k)\| \to \infty$.

To sum up, $\|\Delta e(k)\| \to \infty$ and $\|\Delta z(k)\| = 0$ in Definition 1 hold when $\rho(A_p) > 1$, which implies that the joint attack sequence $\{\Sigma^a(k), a_y(k)\}$ is strictly stealthy. ∎

The joint attack on switching signal and sensor signal is a strictly stealthy one which steers the state to infinity without triggering the alarm of residual-based detector. Comparing with the single attack, one finds that the joint attack is more cunning [17]. Moreover, there is no additional constraint of attacked switching signal $\sigma^a(k)$ when launching the joint attack.

Remark 3: In Theorem 1, a criterion is given for the design of a strictly stealthy attack. It is noted that stability of switched system is determined by both the switching signal and the dynamics of subsystem [28]. This means that $\zeta(k)$ may also diverge when an inappropriate switching signal sequence $\Sigma(k)$ is adopted even if all the subsystems are stable.

IV. Simulation

Consider the switched system with three subsystems

$$A_1 = \begin{bmatrix} -1.49 & -0.12 & -0.43 \\ 0 & 0.99 & -0.08 \\ 1 & 0.82 & 0 \end{bmatrix}, \ B_1 = \begin{bmatrix} 0.1 \\ 0.1 \\ 0.2 \end{bmatrix}$$

$$A_2 = \begin{bmatrix} -0.49 & 0.62 & -0.43 \\ 0 & 1.09 & -0.08 \\ 0.05 & 0.82 & 0 \end{bmatrix}, \ B_2 = \begin{bmatrix} -0.5 \\ -0.3 \\ 0.2 \end{bmatrix}$$

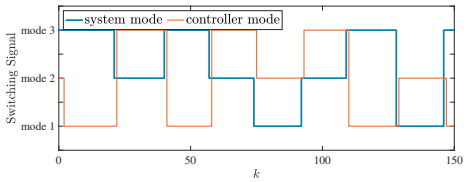

Fig. 2. System mode and controller mode for switched system suffering from attack

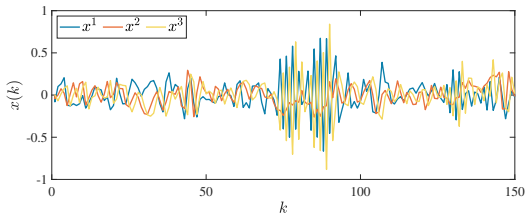

Fig. 3. State evolution for the attack-free case

$$A_3 = \begin{bmatrix} 0.99 & -0.12 & -0.93 \\ -0.20 & -0.09 & -0.75 \\ 0.10 & 0.82 & 0 \end{bmatrix}, \ B_3 = \begin{bmatrix} 0.5 \\ 0.3 \\ -0.2 \end{bmatrix}$$

$$C_1 = \begin{bmatrix} 0.5 & -0.1 & 0.1 \end{bmatrix}$$
$$C_2 = \begin{bmatrix} 0.4 & 0.3 & 0.4 \end{bmatrix}$$
$$C_3 = \begin{bmatrix} -1.5 & -0.3 & -1.5 \end{bmatrix}$$

And the controller gains and estimator gains are

$$K_1 = \begin{bmatrix} -0.4 & 0.6 & -1.6 \end{bmatrix}$$
$$K_2 = \begin{bmatrix} 0.4 & 1.4 & 1.6 \end{bmatrix}$$
$$K_3 = \begin{bmatrix} -1.7 & 1.2 & 1.3 \end{bmatrix}$$

and

$$L_1 = \begin{bmatrix} 0.9 \\ -1 \\ 0.6 \end{bmatrix}, \ L_2 = \begin{bmatrix} 0.1 \\ 1.1 \\ 0.1 \end{bmatrix}, \ L_3 = \begin{bmatrix} 0.5 \\ -0.2 \\ 0.1 \end{bmatrix}$$

Moreover, $W = diag\{0.1^2, 0.1^2, 0.01^2\}$ and $V = diag\{0.1^2\}$. The system mode is shown in Fig. 2 with blue line. Under this switching law, the system state is within a neighborhood of zero due to the existence of process noise, which implies that the switched system without attack is stable. See Fig. 3 for details.

By calculation, we find that $\rho(\mathcal{A}_{1,2}) = 1.3359$, $\rho(\mathcal{A}_{1,3}) = 0.9316$, $\rho(\mathcal{A}_{2,1}) = 1.7399$, $\rho(\mathcal{A}_{2,3}) = 1.3633$, $\rho(\mathcal{A}_{3,1}) = 2.4934$ and $\rho(\mathcal{A}_{3,2}) = 2.9197$. To seek the condition satisfying Proposition 1, the attacked switching modes are chosen as $2, 3, 1$ corresponding to the original modes $1, 2, 3$. Fig. 2 also plots the attacked switching signal $\sigma^a(k)$ with orange line. The corresponding state trajectories are depicted in Fig. 4. It is obvious that the system becomes unstable under switching signal attack. Moreover, we can see from the residual with/without attack in Fig. 5 that the attack is successfully detected via χ^2 detector due to the obvious anomaly of residual signal.

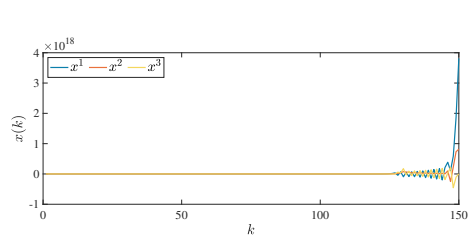

Fig. 4. State trajectories under switching signal attack

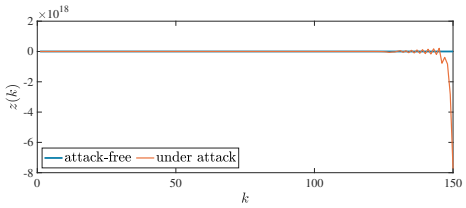

Fig. 5. Estimator residual with/without switching signal attack

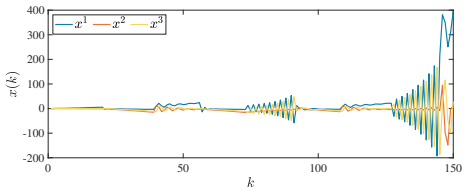

Fig. 6. State trajectories under sensor signal attack

Figs. 6 and 7 demonstrate the state trajectories and estimator residual suffering from sensor signal attack with $\eta = 0.5, M = 1$. We can see that such an attack makes system diverge while bypassing χ^2 detector. Figs. 8 and 9 exhibit the state trajectories and estimator residual under joint attack. The attack data injecting into the sensor signal is illustrated in Fig. 10. It is found that system state diverges while the detector does not alarm, since the estimator residual under attack is the same as the attack-free case. The above simulations verify that the attack presented in this paper is effective. Comparing Fig. 7 with Fig. 9, we can see that the stealthiness of joint attack is higher than that for sensor signal attack as the residual difference caused by joint attack

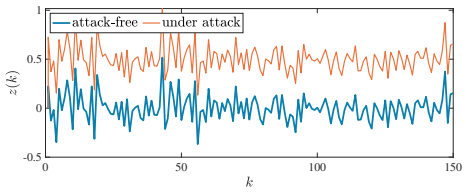

Fig. 7. Estimator residual with/without sensor signal attack

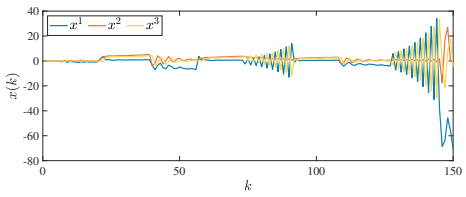

Fig. 8. State trajectories suffering from joint attack

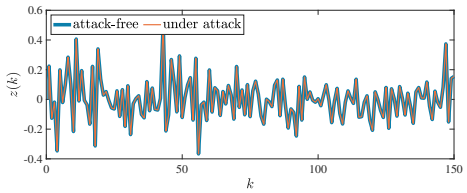

Fig. 9. Estimator residuals under joint attack and attack-free scenarios

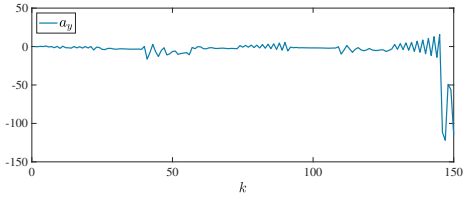

Fig. 10. The attack signal injected into the sensor signal

is significantly smaller than that by sensor signal. Hence, the joint attack is more desirable.

V. CONCLUSION

In this paper, we have addressed the security issue for switched systems where the attack can be injected into sensor signal and/or switching signal. The switching signal attack has been designed without the information of system while causing noticeable effect on the stability, but it could be easily detected. Furthermore, sensor signal attack has been developed which is dangerous since it can bypass the χ^2 detector. However, it fails for SUM detector. Finally, the joint attack on sensor signal and switching signal has been presented to handle the strict detector condition like SUM detector. The joint attack can realize strict stealthiness, that is, the attack can make system diverge while the estimator residual for system under attack keeps unchanged as the attack-free scenario.

VI. REFERENCES

[1] C. Zhou, B. Hu, Y. Shi, Y.-C. Tian, X. Li, and Y. Zhao, "A unified architectural approach for cyberattack-resilient industrial control systems," *Proceedings of the IEEE*, vol. 109, no. 4, pp. 517–541, 2021.

[2] D. Zhang, G. Feng, Y. Shi, and D. Srinivasan, "Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances," *IEEE/CAA Journal of Automatica Sinica*, vol. 8, no. 2, pp. 319–333, 2021.

[3] B. Li, R. Lu, G. Xiao, T. Li, and K.-K. R. Choo, "Detection of false data injection attacks on smart grids: A resilience-enhanced scheme," *IEEE Transactions on Power Systems*, vol. 37, no. 4, pp. 2679–2692, 2022.

[4] Z. Ju, H. Zhang, and Y. Tan, "Distributed deception attack detection in platoon-based connected vehicle systems," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 4609–4620, 2020.

[5] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[6] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, 2017.

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

[8] R. Zhao, Z. Zuo, and Y. Wang, "Event-triggered control for switched systems with denial-of-service attack," *IEEE Transactions on Automatic Control*, vol. 67, no. 8, pp. 4077–4090, 2022.

[9] R. Zhao, Z. Zuo, Y. Wang, and W. Zhang, "Active control strategy for switched systems against asynchronous DoS attacks," *Automatica*, vol. 148, p. 110765, 2023.

[10] Y. Li, Y. Yang, Z. Zhao, J. Zhou, and D. E. Quevedo, "Deception attacks on remote estimation with disclosure and disruption resources," *IEEE Transactions on Automatic Control*, 2022. doi: 10.1109/TAC.2022.3202981.

[11] S. X. Ding, L. Li, D. Zhao, C. Louen, and T. Liu, "Application of the unified control and detection framework to detecting stealthy integrity cyber-attacks on feedback control systems," *Automatica*, vol. 142, p. 110352, 2022.

[12] E. Kung, S. Dey, and L. Shi, "The performance and limitations of ϵ-stealthy attacks on higher order systems," *IEEE Transactions on Automatic Control*, vol. 62, no. 2, pp. 941–947, 2017.

[13] Y. Mo and B. Sinopoli, "False data injection attacks in control systems," *Preprints of the 1st Workshop on Secure Control Systems*, pp. 1–7, 2010.

[14] T.-Y. Zhang and D. Ye, "False data injection attacks with complete stealthiness in cyber-physical systems: A self-generated approach," *Automatica*, vol. 120, p. 109117, 2020.

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

[16] Y. Ni, Z. Guo, Y. Mo, and L. Shi, "On the performance analysis of reset attack in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 65, no. 1, pp. 419–425, 2020.

[17] W. Xu, Z. Wang, L. Hu, and J. Kurths, "State estimation under joint false data injection attacks: Dealing with constraints and insecurity," *IEEE Transactions on Automatic Control*, vol. 67, no. 12, pp. 6745–6753, 2022.

[18] 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, 2021.

[19] D. Mikhaylenko and P. Zhang, "Stealthy local covert attacks on cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 67, no. 12, pp. 6778–6785, 2022.

[20] A.-Y. Lu and G.-H. Yang, "False data injection attacks against state estimation without knowledge of estimators," *IEEE Transactions on Automatic Control*, vol. 67, no. 9, pp. 4529–4540, 2022.

[21] I. Malloci, J. Daafouz, C. Lung, and P. Szczepanski, "Switched system modeling and robust steering control of the tail end phase in a hot strip mill," *IFAC Proceedings Volumes*, vol. 42, no. 17, pp. 386–391, 2009.

[22] Y. Yuan, H. Yuan, L. Guo, H. Yang, and S. Sun, "Resilient control of networked control system under DoS attacks: A unified game approach," *IEEE Transactions on Industrial Informatics*, vol. 12, no. 5, pp. 1786–1794, 2016.

[23] J. Yang, Q. Zhong, K. Shi, and S. Zhong, "Dynamic-memory event-triggered H_∞ load frequency control for reconstructed switched model of power systems under hybrid attacks," *IEEE Transactions on Cybernetics*, 2022. doi: 10.1109/TCYB.2022.3170560.

[24] Z. Sun and S. S. Ge, *Stability Theory of Switched Dynamical Systems*. Communications and Control Engineering, London: Springer London, 2011.

[25] D. Liberzon, *Switching in Systems and Control*. Systems & Control: Foundations & Applications, Boston, MA: Birkhäuser Boston, 2003.

[26] L. Zhang and H. Gao, "Asynchronously switched control of switched linear systems with average dwell time," *Automatica*, vol. 46, no. 5, pp. 953–958, 2010.

[27] J. Hu, J. Shen, and D. Lee, "Resilient stabilization of switched linear control systems against adversarial switching," *IEEE Transactions on Automatic Control*, vol. 62, no. 8, pp. 3820–3834, 2017.

[28] D. Sun and I. Hwang, "Resilient control design for hybrid systems against switching and data injection attacks," in *IEEE 58th Conference on Decision and Control*, pp. 3854–3859, 2019.

[29] H. Kim, P. Guo, M. Zhu, and P. Liu, "Attack-resilient estimation of switched nonlinear cyber-physical systems," in *2017 American Control Conference*, pp. 4328–4333, 2017.

[30] D. Ye and T.-Y. Zhang, "Summation detector for false data-injection attack in cyber-physical systems," *IEEE Transactions on Cybernetics*, vol. 50, no. 6, pp. 2338–2345, 2020.

[31] S. Shi, Z. Shi, and Z. Fei, "Asynchronous control for switched systems by using persistent dwell time modeling," *Systems & Control Letters*, vol. 133, p. 104523, 2019.