2024 European Control Conference (ECC)
June 25-28, 2024. Stockholm, Sweden

Secure State Estimation of Networked Switched Systems under Denial-of-Service Attacks

Qingkai Meng[1], Andreas Kasis[1], Hao Yang[2], Marios M Polycarpou[1]

***Abstract*— This paper studies the problem of secure state estimation of networked switched systems in the presence of denial-of-service (DoS) attacks, as well as disturbances and measurement noise. Firstly, a state transformation rule is designed to partition the original system into two subsystems, facilitating the design of discrete and continuous state observers. Secondly, by modifying the traditional super-twisting sliding-mode method and taking into account the frequency and duration characteristics of DoS attacks, we employ dynamic differential properties between different modes to design a switching law identification strategy. We show that this strategy can accurately estimate the switching state without imposing any requirement on the switching times and sequences. Thirdly, based on the identified activated mode, a set of mode-dependent continuous state sliding-mode observers is designed, that achieves continuous state estimation in finite time. The practicality and applicability of the developed results are validated through numerical simulations.**

I. Introduction

Emerging from the intersection of modern control technology, computer technology, and communication technology, networked control systems (NCSs) exhibit several desirable characteristics, including improved efficiency, reduced costs, enhanced flexibility, and better remote control and monitoring capabilities [1], [2]. They play a vital role in various domains like energy management [3], water distribution [4], and intelligent housing [5]. Physical plants with switching modes can capture the impact of external conditions, jumping parameters, or changing control strategies [6], [7], leading to the emergence and widespread attention of networked switched systems (NSSs) in recent years [8], [9].

Despite significant progress, the integration of information and physical space presents new challenges for NCSs. The complex system structure magnifies the impact of external disturbances and uncertainties on perception, communication, and control. In addition, the open communication environment heightens susceptibility to network attacks. Ensuring NCS security against these challenges is crucial, with *secure state estimation* emerging as a key research focus [10].

As one kind of the prevalent cyber-attacks, denial-of-service (DoS) attacks operate without the need for prior system knowledge. They undermine the connectivity of communication networks, consequently impinging upon the exchange of information and real-time data flow [11]. To cope with secure state estimation under DoS attacks, extensive results can be found for NCSs, such as the zero-sum game strategy [12], the resilient estimator [13], and the neural-network-based method [14]. However, in the case of NSSs are considered, to the best of the authors' knowledge, there are currently no results concerning the secure state estimation against DoS attacks. The main challenges to achieve the secure state estimation of NSSs are: i) The transmitted measurement data may exhibit delays and packet loss. ii) The unknown timing and order of switching laws as well as the false switching dynamics induced by DoS attacks increase the design complexity. iii) The presence of measurement noise and dynamic disturbances makes the known information available for state estimation less reliable.

Contribution: Inspired by the above issues, this paper studies the secure state estimation for NSSs in the presence of DoS attacks, dynamic disturbances and measurement noise. Firstly, we analyze the dynamic difference between the different modes under bounded uncertainty assumptions. Based on the mode identification condition, an augmented super-twisting sliding-mode (ASSM) observer is proposed, which is used for constructing a discrete state observer. Secondly, with partially observable continuous states, based on the estimated activated mode information, we design a group of mode-dependent ASSM observers to estimate the observable states. Then, we estimate the continuous state in finite time, by suitably designing a correction term utilizing an appropriate state transformation. Finally, the theoretical results are verified through a numerical simulation.

Notation: Denote the sets of real and integer numbers by $\mathbb{R}$ and $\mathbb{N}$, respectively. A subset of $\mathbb{R}$ (or $\mathbb{N}$) satisfying condition $(\cdot)$ is denoted by $\mathbb{R}_{(\cdot)}$ (or $\mathbb{N}_{(\cdot)}$). For a matrix A, denote its maximum and minimum eigenvalues by $\lambda_{\max}(A)$ and $\lambda_{\min}(A)$, respectively. Denote the matrix whose rows span the null space of A by $A^{\perp}$ and the pseudo-inverse of A by $A^{\dagger}$. Given a function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}^n$ and a time interval $[0, \infty)$, we denote the $\mathcal{L}_\infty$ norm of $f(\cdot)$ on $[0, \infty)$ by $\|f\|_\infty := \text{ess sup}_{s\in[0,\infty)} \|f(s)\|$. A function $f(\cdot)$ is called continuous from the right at point c, if $\forall \varepsilon \in \mathbb{R}_{>0}$, $\exists \delta \in \mathbb{R}_{>0}$ such that for all x satisfying $c < x < c+\delta$, the value of $f(x)$ satisfies $|f(x) - f(c)| < \varepsilon$. For two functions$f(x), g(x)$, if $\lim_{x\to 0} \frac{f(x)}{g(x)} = 0$, we call $f(x)$ is the infinitesimal of higher order of $g(x)$ at 0, denoted by $f(x) = o(g(x))$.

II. Problem formulation

A. System description

Consider a NSS, whose physical plant is described as a switched linear system with N modes in the form of

$$\begin{aligned} \dot{x}(t) =& A_{\sigma(t)}x(t) + B_{\sigma(t)}u(t) + Dd(t), \\ y(t) =& Cx(t) + E\omega(t), \end{aligned} \tag{1}$$

where $\sigma(t) : [0, \infty) \to S := \{1, 2, \cdots, N\}$ denotes the switching signal that is a piece-wise constant function continuous from the right, and N is the number of switching modes. A switching sequence is defined as

$$\Sigma := \{(\sigma_0, s_0), (\sigma_1, s_1), \cdots, (\sigma_i, s_i), \cdots\},$$

where s_i denotes the ith switching instant and $\sigma_i := \sigma(s_i) \in S$. For the estimation problem, we consider $\sigma(t)$ as a discrete state to estimate, while $x(t) \in \mathbb{R}^n$ is the continuous state vector to estimate, $u(t) \in \mathbb{R}^m$ is the known control input, and $y(t) \in \mathbb{R}^p$ is the measurement output. Variables $d(t) \in \mathbb{R}^l$ and $\omega(t) \in \mathbb{R}^s$ represent the unknown disturbance and noise presented in the actuator and sensor channels. Matrices $A_i \in \mathbb{R}^{n\times n}$, $B_i \in \mathbb{R}^{n\times m}$, $i \in S$, $C \in \mathbb{R}^{p\times n}$, $D \in \mathbb{R}^{n\times l}$, and $E \in \mathbb{R}^{p\times s}$ are known with appropriate dimensions. For convenience, for the rest of the paper we do not explicitly state the time argument unless required after (1).

Consider a periodic sampler that quantizes the continuous measurement $y(t)$ into a zero-order holding signal. Denote $\{t_k\}_{k\in\mathbb{N}_{\geq 0}}$ as the set of sampling instants satisfying

$$\delta_{\min} \leq t_{k+1} - t_k =: \delta \leq \delta_{\max},\ t_0 = 0, \tag{2}$$

where $\delta_{\min}, \delta_{\max} \in \mathbb{R}_{>0}$ denote respectively the minimum and maximum bounds of the unknown sampling period δ. Subsequently, the sampling signal $y(t_k)$ is transmitted to the estimator via a communication network, which may be subject to DoS attacks, as depicted in Fig. 1.

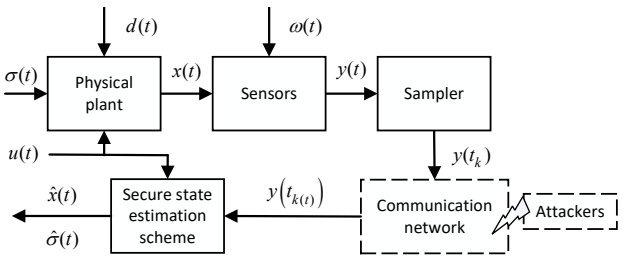

Fig. 1. The secure state estimation framework for a NSS under DoS attacks.

To characterize the switching law $\sigma(t)$, we introduce the following definition about minimum dwell time.

***Definition** 1 ([15]):* For the switching signal $\sigma(t)$ with the switching sequences in terms of time $\{s_k\}_{k\in\mathbb{N}_{\geq 0}}$, the positive constant $\tau_a := \min_{k\in\mathbb{N}_{\geq 0}}(s_{k+1} - s_k)$ is called the *minimum dwell time*.* ■

The following assumptions are imposed to facilitate the design of the secure state estimator.

***Assumption** 1:* The system (1) satisfies:

(i) The state $x(t)$ evolves in a bounded region, $\forall t \geq 0$.
(ii) There exists constants $\bar{d}, \hat{d}, \bar{\omega}, \hat{\omega} \in \mathbb{R}_{>0}$ such that $\|d\|_\infty \leq \bar{d}$, $\|\dot{d}\|_\infty \leq \hat{d}$, $\|\omega\|_\infty \leq \bar{\omega}$, $\|\dot{\omega}\|_\infty \leq \hat{\omega}$.
(iii) $\mathrm{rank}(CD) = \mathrm{rank}(D) = l$.
(iv) The minimum dwell time $\tau_a > \delta_{\max}$. ■

***Remark** 1:* The first and second conditions concern physical limitations and safety constraints in practical systems, necessitating bounded system states, disturbances, and noise. When A_i is stable, $\forall i \in S$, (i) is implied by (ii) if the control input u is either bounded or represents state feedback with bounded gain. The third point is a precondition to design a sliding mode observer which rejects uncertainties d. This means that the output is sensitive to the effect of disturbances and has been widely utilized [16]. The last point guarantees that at most one switch occurs during one sampling period. This prevents unnecessary switches, avoiding Zeno behavior by ensuring a finite number of switches over any finite time. Notably, no assumptions about the timing and order of switching laws are required. This, coupled with false switching dynamics induced by DoS attacks, makes direct ultilization of the existing discrete-time estimation algorithms, e.g., [17], impractical for state and/or disturbance estimation. ■

B. Modelling DoS attacks

Considering DoS attacks on the measurement channel, data transmission service is denied upon occurrence of an attack. Inspired by [18], DoS attacks are modeled based on both attack frequency and duration. Denote the attack instant sequence as $h_n, n \in \mathbb{N}\geq 0$, then within the time interval of the nth DoS attack

$$H_n := \{h_n\} \cup (h_n, h_n + \tau_n),$$

the communication is interrupted, with the length of the nth DoS attack $\tau_n \in \mathbb{R}_{\geq 0}$. For $t \geq \tau \in \mathbb{R}_{\geq 0}$, denote

$$\Xi(\tau, t) := \bigcup_{n\in\mathbb{N}_{\geq 0}} H_n \bigcap [\tau, t],\ \Theta(\tau, t) := [\tau, t] \setminus \Xi(\tau, t).$$

Specifically, for the interval $[\tau, t]$, $\Xi(\tau, t)$ and $\Theta(\tau, t)$ represent the sets of time instants where communication is denied and allowed, respectively. Let $\Delta_n := h_{n+1} - h_n > \tau_n$, $n \in \mathbb{N}_{\geq 0}$, denote the time elapsing between any two successive DoS attacks. The severity of a DoS attack can be described by its frequency and duration length.

***Assumption** 2:* For DoS attacks, there exist known positive constants $\tau_{\max} < \tau_a$ and $\tau_{\min} > \delta_{\max}$ such that

$$\sup_{n\in\mathbb{N}_{\geq 0}}\{\tau_n\} \leq \tau_{\max},\ \inf_{n\in\mathbb{N}_{\geq 0}}\{\Delta_n\} \geq \tau_{\min}.$$ ■

Based on the above, for each $t \in \mathbb{R}_{\geq 0}$, the measurement output can be represented as $y(t_{\hat{k}(t)})$, where

$$\hat{k}(t) = \begin{cases} -1, & \text{if } \Theta(0,t) = \emptyset, \\ \sup\{k \in \mathbb{N}_0 \,|\, t_k \in \Theta(0,t)\}, & \text{otherwise.} \end{cases}$$

In this form, $\hat{k}(t)$ represents the last update instant when the communication transmission is successful. That is the measurement signal will maintain the data of the last successful update instant. Without loss of generality, we set $t_{-1} = 0$.

C. Problem statement

This subsection presents a statement of the problem considered in this paper, which is provided below.

***Problem** 1:* Under Assumptions 1-2, design an observer for system (1), which in the presence of DoS attacks:

(i) Identifies the switching law $\sigma(t)$ in finite time;
(ii) Estimates the continuous state $x(t)$ in finite time; ■

Property (i) is required to identify the activated mode, which is a prerequisite to determine the dynamics used for the continuous state estimation. Followed by the identified activated mode, (ii) requires an estimation scheme of the system's continuous state. Furthermore, (i) and (ii) should be accomplished while tolerating bounded disturbances and measurement noise, as well as handling DoS attacks with known frequency and duration bounds.

III. Switching law identification

In this section a novel discrete state observer based on the super-twisting second-order sliding-mode technique is designed to estimate the switching signal $\sigma(t)$ in finite time.

A. Transformed system and preliminary assumptions

The transformed state coordinates are introduced to decouple the unknown disturbance $d(t)$ from the system (1):

$$T = \begin{bmatrix} D^{\perp} \\ (CD)^{\dagger}C \end{bmatrix},\ U = \begin{bmatrix} (CD)^{\perp} \\ (CD)^{\dagger} \end{bmatrix},$$

where $T \in \mathbb{R}^{n\times n}$ and $U \in \mathbb{R}^{p\times p}$ are non-singular matrices. This transformation is feasible due to Assumption 1 (iii). Specifically, we define the transformed state as

$$\bar{x}(t) = [x_1^{\top}(t)\ x_2^{\top}(t)]^{\top} = Tx(t),$$

where $x_1(t) \in \mathbb{R}^{n-m}$ and $x_2(t) \in \mathbb{R}^m$. Similarly, we define the transformed output as

$$\bar{y} = [y_1^{\top}(t)\ y_2^{\top}(t)]^{\top} = Uy(t),$$

where $y_1(t) \in \mathbb{R}^{p-m}$ and $y_2(t) \in \mathbb{R}^m$. In the new domain, one can obtain the following transformed dynamics

$$\dot{x}_1(t) = A1_{\sigma(t)}x_1(t) + A2_{\sigma(t)}x_2(t) + B1_{\sigma(t)}u(t), \tag{3a}$$
$$\dot{x}_2(t) = A3_{\sigma(t)}x_1(t) + A4_{\sigma(t)}x_2(t) + B2_{\sigma(t)}u(t) + d(t), \tag{3b}$$
$$y_1(t) = C1x_1(t) + E1\omega(t), \tag{3c}$$
$$y_2(t) = x_2(t) + E2\omega(t), \tag{3d}$$

with the implicit definition of matrices $A1_{\sigma(t)}$, $A2_{\sigma(t)}$, $A3_{\sigma(t)}$, $A4_{\sigma(t)}$, $B1_{\sigma(t)}$, $B2_{\sigma(t)}$, $C1$, $E1$ and $E2$.

The error between the current measurement and actual output is

$$e_{d,y_2}(t) := y_2(t_{\hat{k}(t)}) - y_2(t).$$

Define $\kappa(t) := t - t_{\hat{k}(t)}$. Using Taylor's series expansion, the delayed signal $y_2(t_{\hat{k}(t)})$ can be written as

$$y_2(t_{\hat{k}(t)}) = y_2(t-\kappa(t)) = y_2(t) - \dot{y}_2(t)\kappa(t) + \hbar(t),$$

where $\hbar(t)$ represents the higher order terms of the Taylor's series expansion. According to the sampling mechanism (2) and Assumption 2, it follows that $\kappa(t) \le \tau_{\max} + \delta_{\max}$ and

$$\|e_{d,y_2}(t)\|_{\infty} \le (\tau_{\max} + \delta_{\max})\|\dot{y}_2(t)\|_{\infty}, \tag{4}$$

where $\|\dot{y}_2(t)\|_{\infty}$ satisfies

$$\|\dot{y}_2(t)\|_{\infty} \le \|\dot{x}_2\|_{\infty} + \lambda_{\max}(E2)(\tau_{\max} + \delta_{\max})\hat{\omega}.$$

To guarantee the distinguishability between the modes in S, the following assumption is required.

Assumption 3: There exists a known positive constant $\delta_1 < \tau_a/2$ such that, for any $t > \delta_1$, $\forall i, j \in S$, $i \neq j$:

$$\int_{t-\delta_1}^{t} \|\phi_{i,j}(\tau)\|d\tau > \int_{t-\delta_1}^{t} \|\phi_{i,i}(\tau)\|d\tau \tag{5}$$

where

$$\begin{aligned}\phi_{i,j} :=& A4_i\xi_2(t) - A3_jx_1(t) + (A4_i - A4_j)x_2(t) \\ &+ (B2_i - B2_j)u(t) - d(t).\end{aligned}$$

with $\xi_2(t) := e_{d,y_2}(t) + E2\omega(t)$. ■

Remark 2: The intuition behind Assumption 3 is that when a mode change occurs, after a period of time it enables larger changes in $\phi_{i,j}$ than in $\phi_{i,i}$. To identify the modes of the plant, the dynamic difference of modes should be considered. Based on whether the error of dynamics is related, the term $\phi_{i,j}$ can be divided into two parts:

$$\begin{aligned}a(t) =& (A4_i - A4_j)x_2(t) + (B2_i - B2_j)u(t), \\ b(t) =& -A3_jx_1(t) + A4_i\xi_2(t) - d(t).\end{aligned}$$

From Assumption 1 and (4), one can deduce that $\|b(t)\| \le \Pi_1(t)$, where Π_1 is a known positive function. We can see that $\|a(t)\| \equiv 0$ if $i = j$ while $\|a(t)\| \ge 0$ if $i \neq j$. When there exists $\delta_1 < \tau_a$ such that $\int_{t-\delta_1}^{t} \|\phi_{i,j}\| \ge \Pi_2(t), i \neq j$ and $\Pi_2(t) > \delta_1\Pi_1(t)$, condition (5) is satisfied. ■

B. Mode identification under DoS attacks

To estimate the switching law $\sigma(t)$, consider a set of mode-dependent sliding-mode observers in the form of

$$\dot{\hat{x}}_{2,i}(t) = A4_i\hat{x}_{2,i}(t) + B2_iu(t) + v_i(t),\ i \in S, \tag{6}$$

where $\hat{x}_{2,i}$ is the estimated state of x_2 in the ith observer. Denote the ideal estimation error by $e_{2,i}(t) := \hat{x}_{2,i}(t) - x_2(t)$ and the actual estimation error by $\pi_{2,i}(t) = \hat{x}_{2,i}(t) - y_2(t_k)$. The correction terms $v_i, i \in S$ are designed as

$$\begin{aligned}v_i(t) &= -k_1\lceil\pi_{2,i}(t)\rfloor^{\frac{1}{2}} - A4_i\pi_{2,i}(t) + v_{i,1}(t) \\ \dot{v}_{i,1}(t) &= -k_2\mathrm{sign}(\pi_{2,i}(t)),\end{aligned} \tag{7}$$

where $k_1, k_2 \in \mathbb{R}_{>0}$ are design parameters and $\lceil\pi_{2,i}(t)\rfloor^{\frac{1}{2}} := \left[\lceil\pi_{2,i1}(t)\rfloor^{\frac{1}{2}}, \cdots, \lceil\pi_{2,im}(t)\rfloor^{\frac{1}{2}}\right]^{\top}$ with $\lceil\pi_{2,ij}(t)\rfloor^{\frac{1}{2}} := |\pi_{2,ij}(t)|^{\frac{1}{2}}\mathrm{sign}(\pi_{2,ij}(t))$, $j = 1, \cdots, m$.

Theorem 1: Consider the NSS (1) satisfying Assumptions 1-3 and the observer (6)-(7) with

$$k_1 > 0,\ k_2 > \phi_{\max}, \tag{8}$$

where $\phi_{\max} := \max_{i,j\in S}\left\|\dot{\phi}_{i,j}\right\|_{\infty}$. The discrete observer

$$\hat{\sigma}(t) = \arg\min_{i} \int_{t-\delta_1}^{t} \|v_{i,1}(\tau)\|d\tau \tag{9}$$

accurately estimates $\sigma(t)$ in each interval $[s_k + T_e, s_{k+1})$, where $\delta_1 < T_e < \tau_a - \delta_1$. ■

Proof: Assume that, during the interval $[s_k, s_{k+1})$ for some $k \in \mathbb{N}_{\ge 0}$, the jth mode of the plant is activated, by using (3b) and (6), the dynamics of $e_{2,i}$ satisfy

$$\begin{aligned}\dot{e}_{2,i}(t) =& A4_i\left(e_{2,i}(t) - \pi_{2,i}(t)\right) - A3_jx_1(t) - d(t) \\ &+ (A4_i - A4_j)x_2(t) + (B2_i - B2_j)u(t) \\ &- k_1\lceil\pi_{2,i}(t)\rfloor^{\frac{1}{2}} + v_{i,1}(t) \\ =& \phi_{i,j} + v_{i,1}(t) - k_1\lceil\pi_{2,i}(t)\rfloor^{\frac{1}{2}}\end{aligned} \tag{10}$$

Define variable $v_{i,2}(t) := \phi_{i,j}(t) + v_{i,1}(t)$. Then,

$$\dot{v}_{i,2}(t) = \dot{\phi}_{i,j} - k_2\mathrm{sign}(\pi_{2,i}). \tag{11}$$

The following result, referred to Claim 1, can be deduced.

Claim 1. With the observer (6)-(7) satisfying (8), the error $e' := [e_{2,i}; v_{i,2}], i \in S$, enters the set $\Omega_e := \{e' \in \mathbb{R}^{2m} \mid \|e_{2,i}(t)\|_{\infty} < \|\xi_2(t)\|_{\infty}, v_{i,2} = 0\}$ in finite time. □

To deduce this, define the pth element of $e_{2,i}$ ($v_{i,2}$) as $e_{2,ip}$ ($v_{ip,2}$), $p = 1, \cdots, m$, and introduce an auxiliary variable

$$\zeta_{ip}^{\top} := [\zeta_{ip,1}, \zeta_{ip,2}] = \left[\lceil e_{2,ip}(t)\rfloor^{\frac{1}{2}}, v_{ip,2}(t)\right].$$

Then consider the quadratic function

$$V_{ip}(\zeta_{ip}) = \zeta_{ip}^{\top} P_{ip} \zeta_{ip},$$

with $P_{ip} := \mathrm{diag}\{p_{ip,1}, p_{ip,2}\} \in \mathbb{R}^{2\times 2}$ a constant, symmetric and positive definite matrix, as a candidate Lyapunov function, where $p_{ip,1}, p_{ip,2} > 0$. It follows that

$$\lambda_{\min}\{P_{ip}\}\|\zeta_{ip}\|^2 \le V(\zeta_{ip}) \le \lambda_{\max}\{P_{ip}\}\|\zeta_{ip}\|^2. \quad (12)$$

With this form, it has been proven in [19] that, when $\xi_2(t) \equiv 0$ and $\phi_{i,j} \equiv 0$, there exists a positive definite and symmetric matrix Q_{ip} such that

$$A_{ip}^{\top} P_{ip} + P_{ip} A_{ip} = -Q_{ip}, A_{ip} := \begin{bmatrix} -\frac{1}{2}k_1 & \frac{1}{2} \\ -k_2 & 0 \end{bmatrix}$$

where A_{ip} such that $\dot{\zeta}_{ip} = \frac{1}{|\zeta_{ip,1}|} A_{ip}\zeta_{ip}$.

Taking the derivative of V_{ip} along (10)-(11) yields

$$\dot{V}_{ip} = \dot{\zeta}_{ip}^{\top} P_{ip}\zeta_{ip} + \zeta_{ip}^{\top} P_{ip}\dot{\zeta}_{ip},$$

where $\dot{\zeta}_{ip}$ is given as

$$\dot{\zeta}_{ip} = \begin{bmatrix} \frac{1}{2}\frac{1}{|e_{2,ip}|^{\frac{1}{2}}}\left(\zeta_{ip,2} - k_1 \lceil \pi_{2,ip} \rfloor^{\frac{1}{2}}\right) \\ \dot{\phi}_{ip,j} - k_2 \mathrm{sign}(\pi_{2,ip}) \end{bmatrix}.$$

Claim 1 is implied by that when $|e_{2,ip}(t)| > \|\xi_2(t)\|_\infty$ and $v_{ip,2} \neq 0$, then $\dot{V}_{ip}(\zeta_{ip}) < -\alpha V_{ip}^{\frac{1}{2}}(\zeta_{ip})$, for some $\alpha > 0$ and all $i \in S, p = 1, \cdots, m$. We prove this in two cases.

Case (i): $e_{2,ip}(t) > \|\xi_2(t)\|_\infty$ and $v_{ip,2} \neq 0$. In this case, $\pi_{2,ip} > 0$ and thus

$$\dot{\zeta}_{ip} = \begin{bmatrix} \frac{1}{2}\frac{1}{|e_{2,ip}|^{\frac{1}{2}}}\left(\zeta_{ip,2} - k_1 \left(e_{2,ip} - \xi_{2,p}\right)^{\frac{1}{2}}\right) \\ \dot{\phi}_{ip,j} - k_2 \end{bmatrix}.$$

Therefore, $\dot{V}_{ip}$ satisfies

$$\dot{V}_{ip} \le \frac{1}{|e_{2,ip}|^{\frac{1}{2}}} \zeta_{ip}^{\top}\left[W_{ip}^{\top} P_{ip} + P_{ip} W_{ip}\right]\zeta_{ip},$$

where $W_{ip} := A_{ip} + N_{ip}(t)$ is defined as

$$\begin{bmatrix} -\frac{1}{2}k_1\left(1 - \frac{1}{|e_{2,ip}|}\|\xi_2(t)\|_\infty^{\frac{1}{2}}\right) & \frac{1}{2} \\ -k_2 + \dot{\phi}_{ip,j} & 0 \end{bmatrix}.$$

Hence, when P is positive definite, $\dot{V}_{ip}$ is negative definite if and only if $A_{ip} + N_{ip}(t)$ is Hurwitz. This is implied by

$$k_1 > 0, k_2 > \|\dot{\phi}_{i,j}\|_\infty. \quad (13)$$

Case (ii): $e_{2,ip}(t) < -\|\xi_2(t)\|_\infty$ and $v_{ip,2}(t) \neq 0$. In this case, $\pi_{2,ip} < 0$ and thus along the proof in case (i), when (13) is satisfied, it follows that the matrix

$$\begin{bmatrix} -\frac{1}{2}k_1\left(1 + \frac{1}{|e_{2,ip}|}\|\xi_2(t)\|_\infty^{\frac{1}{2}}\right) & \frac{1}{2} \\ -k_2 - \dot{\phi}_{ip,j} & 0 \end{bmatrix}$$

is Hurwitz. Therefore, it holds that

$$\dot{V}_{ip} \le -|e_{2,ip}|^{-\frac{1}{2}} \zeta_{ip}^{\top} Q_{ip}\zeta_{ip}.$$

for the above two cases. Moreover, from (12) and the fact that $|\zeta_{ip,1}|^{\frac{1}{2}} \le \|\zeta_{ip}\| \le \lambda_{\min}^{-\frac{1}{2}}\{P_{ip}\} V_{ip}^{\frac{1}{2}}$, it follows that $\dot{V}_{ip} \le -\alpha V_{ip}^{\frac{1}{2}}$, where α is given by

$$\alpha := \frac{\lambda_{\min}^{\frac{1}{2}}\{P_{ip}\}\lambda_{\min}\{Q_{ip}\}}{\lambda_{\max}\{P_{ip}\}}.$$

Therefore, a trajectory starting at the initial estimation error $e_{ip}(0) := [e_{2,ip}(0), v_{ip,2}(0)]$ will converge to the region Ω_e in some finite time smaller than

$$T_e \le \frac{2}{\alpha} V_{ip}^{\frac{1}{2}}(e_{ip}(0)).$$

From the above, one can see that the upper bound T_e relies on the initial error $e_{ip}(0)$ and the eigenvalues of matrices P_{ip}, Q_{ip}, which can be adjusted by parameters k_1 and k_2. Therefore, the finite convergence time $T_e < \tau_a - \delta_1$ can be set as small as required by selecting the appropriate k_1 and k_2 in condition (8). Based on Claim 1, one has that $v_{i,1}(t) = -\phi_{i,j}(t)$ since $v_{i,2} = 0$ if $T_e > \delta_1$. From Assumption 3, one gets

$$\int_{t-\delta_1}^{t} \|v_{i,1}(\tau)\| d\tau \ge \int_{t-\delta_1}^{t} \|v_{j,1}(\tau)\| d\tau, i \neq j.$$

As a result, the proposed estimation logic (9) provides an exact estimation of the switching law $\sigma(t)$ after the transient time $T_e \ge \delta_1$. This completes the proof. ■

Theorem 1 shows the effectiveness of the ASSM observer, which improves the robustness of the super-twisting sliding-mode under measurement noise. From (i) in Assumption 1, one can see that $\phi_{\max}$ exists and its upper bound can be suitably calculated. Based on Assumption 3, the structure of the discrete state observer requires a period of time δ_1 to distinguish the difference between the integration of different modes. The selection of gains k_1, k_2 is also in order to satisfy the condition $T_e < \tau_a/2$. This guarantees the finite time identification of the switching law.

IV. Continuous State Estimation

After obtaining the activated mode index, continuous state estimation can be achieved by designing an observer for the activated subsystem. However, due to the finite time required for mode identification, we need to address the continuous state estimation problem in segments. This necessitates the design of mode-dependent observers in the manner:

$$\begin{aligned} &\dot{\hat{x}}_{1,i}(t) = A1_i\hat{x}_{1,i}(t) + A2_i\hat{x}_2(t) + B1_i u(t),\ t \in [\hat{s}_{k-1}, \hat{s}_k), \\ &\hat{x}_{1,i}(\hat{s}_k) = \hat{x}_1(\hat{s}_k^-) - \eta^k,\ k \in \mathcal{N}_{\ge 1}, \end{aligned} \quad (14)$$

with

$$\hat{x}_1(t) = \begin{cases} \hat{x}_{1,\hat{\sigma}(\hat{s}_{k-1}+T_e)}(t), & \text{if } t \in [\hat{s}_{k-1} + T_e, \hat{s}_k) \\ \hat{x}_1(\hat{s}_{k-1}^-), & \text{if } t \in [\hat{s}_{k-1}, \hat{s}_{k-1} + T_e) \end{cases},$$

where η^k is a correction term that will be designed below, $\hat{s}_k := s_k + T_e$, and $\hat{s}_k^- := \lim_{\varepsilon\to 0}(\hat{s}_k - \varepsilon)$.

Define the estimated error as $e_1(t) := \hat{x}_1(t) - x_1(t)$, the mode-dependent errors as $e_{1,i} := \hat{x}_{1,i} - x_1, i \in S$, and the output error as $e_{y_1,i} = C1\hat{x}_{1,i}(t) - y_1(t) = C1e_{1,i}(t), i \in S$. It should be mentioned that for each mode, the observable state is determined by the following observability matrix

$$G_i := \left[C1,\ C1A1_i,\ \cdots,\ C1A1_i^{n-m-1}\right]^{\top}.$$

According to [20], for observability, we assume there exists at least $\gamma_k \in \mathbb{N}$ switches such that the kernel space

$\mathrm{Ker}(G_{\sigma(s_{k-\gamma_k-1})} \cup \cdots \cup G_{\sigma(s_{k-1})}) = 0$. In the following, we design observers to estimate the observable part of $e_{1,i}$ at time $\hat{t}_k^-$, $\forall i \in S$. Select matrices Z_i^k (respectively W_i^k) such that their columns are an orthonormal basis of $\mathrm{Im}(G_i^\top)$ (respectively $\mathrm{Ker}(G_i)$). As a result, we denote

$$z_i(t) = (Z_i^k)^\top e_{1,i}(t),\ w_i(t) = (W_i^k)^\top e_{1,i}(t),$$
$$V_i(Z_i^k)^\top = (Z_i^k)^\top A1_i,\ R_i(Z_i^k)^\top = C1,$$

where V_i, R_i are matrices with proper dimension, and $z_i(t) \in \mathbb{R}^{l_i}$ is the observable part of $e_{1,i}$. Define

$$\bar{G}_i := \left[R_i,\ R_iV_i,\ \cdots,\ R_iV_i^{l_i-1}\right]^\top,$$

which satisfies $\mathrm{rank}(\bar{G}_i) = l_i$ for some $l_i \leq n-m$.

Therefore, the observable state dynamics satisfy

$$\dot{z}_i(t) = V_iz_i(t),\ t \in [\hat{s}_{k-1}, s_k),$$
$$e_{y_1,i}(t) = R_iz_i(t).$$

The proposed sliding mode observer satisfies

$$\dot{\hat{z}}_i(t) = V_i\hat{z}_i + \mu_i, \forall t \in (\hat{s}_{k-1}, \hat{s}_k), \hat{z}_i(\hat{s}_{k-1}) = 0, \quad (15)$$

for each $i \in S$, where

$$\begin{aligned}\mu_i(t) &= -k_3\lceil\pi_{1,i}(t)\rfloor^{\frac{1}{2}} - L_i\pi_{1,i}(t) + \mu_{i,1}(t),\\ \dot{\mu}_{i,1}(t) &= -k_4\mathrm{sign}(\pi_{1,i}(t)),\end{aligned} \quad (16)$$

where k_3, k_4, $L_i \in \mathbb{R}^{l_i\times(n-m)}$, $i \in S$, are observer gains to design, and $\pi_{1,i}(t) = (Z_i^k)^\top\left(C1\hat{x}_{1,i}(t) - y_1(t_{\hat{k}(t)})\right)$. The above observer aims to render the observable part error z_i converge to zero. We then present the procedure to compute η^k based on the estimated partly observable state. To approximate the estimation error at time t_k^-, the following state transition matrix is used:

$$\begin{aligned}\Phi(\hat{t}_k^-, \hat{t}_j + T_e) :=& e^{A1_{\hat{\sigma}(\hat{s}_{k-1}+T_e)}\Delta_k}e^{A1_{\hat{\sigma}(\hat{s}_{k-2}+T_e)}\Delta_{k-1}}\\ &\cdots e^{A1_{\hat{\sigma}(\hat{s}_j+T_e)}(\Delta_{j+1}-T_e)},\ j<k,\end{aligned}$$

where the switching period is $\Delta_k = \hat{s}_k - \hat{s}_{k-1}$. Introduce

$$\Omega^k = \begin{bmatrix}(\Theta^{k,k})^\top\Phi(\hat{s}_k^-, \hat{s}_{k-1}+T_e)Z_{\hat{\sigma}(\hat{s}_{k-1}+T_e)}\hat{z}_i(\hat{s}_{k-1}+T_e)\\ \vdots\\ (\Theta^{k-\gamma_k,k})^\top\Phi(\hat{s}_k^-, \hat{s}_{k-\gamma_k-1+T_e}+T_e)Z_{\hat{\sigma}(\hat{s}_{k-\gamma_k-1}+T_e)}\\ \cdot\hat{z}_i(\hat{s}_{k-\gamma_k-1}+T_e)(\hat{s}_{k-\gamma_k-1}+T_e)\end{bmatrix}$$

where $\Theta^{j,k}$ is such that, $\forall k \geq \gamma_1+1$, $\forall j = k-\gamma_k, \cdots, k$

$$\mathrm{Im}(\Theta^{j,k}) = \mathrm{Im}\left(\Phi(\hat{s}_k^-, \hat{s}_j^-))W^j_{\hat{\sigma}(\hat{s}_{j-1}+T_e)}\right)^\perp$$
$$\mathrm{Im}(\Theta^{k,k}) = \mathrm{Im}\left(W^k_{\hat{\sigma}(\hat{s}_{k-1}+T_e)}\right)^\perp.$$

Therefore, the correction vector is defined as

$$\eta^k = (\Theta^{k,k}\cdots, \Theta^{k-\gamma_k,k})^{\top\dagger}\Omega^k. \quad (17)$$

Based on the above observers, the estimated state is

$$\hat{x}(t) = T^{-1}\left[\hat{x}_1(t),\ \hat{x}_2(t)\right]^\top. \quad (18)$$

Below, we present our main result regarding the finite time estimation of the continuous states x.

***Theorem** 2:* Consider the NSS described by (1) and let Assumptions 1-3 hold. Then, the observer (14)-(18) provides an estimate $x(t)$ that satisfies

$$\|\hat{x}(t) - x(t)\| \leq o(\tau_{\max} + \delta_{\max}),\ \hat{s}_{k-1} + T_e \leq t \leq s_k,$$

if we set $V_i - L_i$ as a stable matrix, $k_3 > 0$, and $k_4 > \max_{i\in S}\lambda_{\max}(L_i(Z_i^k)^\top)\|e_{d,y_1}(t)\|_\infty + \lambda_{\max}(E_1)\hat{\omega}$. ■

Proof: According to Theorem 1, the discrete state observer $\hat{\sigma}$ provides a finite time estimate of σ, i.e.,

$$\hat{\sigma}(t) = \sigma_k, \hat{s}_{k-1} + T_e \leq t \leq s_k, k = 1, 2, \cdots.$$

Without loss of generality, we assume that $\sigma_k = i$. From (3a), (3c) and (14), the observation error dynamics are

$$\begin{aligned}\dot{z}_{1,i}(t) =& (S_i - L_i)z_{1,i} + \mu_{i,1} - k_3\lceil\pi_{1,i}(t)\rfloor^{\frac{1}{2}}\\ &+ \underbrace{L_i(Z_i^k)^\top(e_{d,y_1}(t) + E1\omega(t))}_{\psi_i}.\end{aligned}$$

Define variable $\mu_{i,2}(t) := \psi_i(t) + \mu_{i,1}(t)$, and with the same process as in proof of Theorem 1, we can conclude that under the observers (14)-(16), the estimation error $e' := [z_i; \mu_{i,2}], i \in S$, enters the set $\Omega_e := \{e' \in \mathbb{R}^{2(l_i))} \mid \|z_i(t)\|_\infty < \|\xi_1(t)\|_\infty, \mu_{i,2} = 0\}$ in finite time and

$$\|e_1(s_k)\| \leq \sum_{q=k-\gamma_k}^{k} H^{q,k}e_{z,\sigma(s_q)}(\hat{s}_{q-1}+T_e) \leq o(\tau_{\max}+\delta_{\max}).$$

Moreover, it follows from Theorem 1 that $e_2 \leq o(\tau_{\max} + \delta_{\max})$. This completes the proof. ■

V. Simulations

In this section we validate our analytic results with a numerical simulation. Consider a NSS in the form of (1) with three modes, whose system matrices are given as follows.

$$A_1 = \begin{bmatrix}-1.5 & -1.5 & 0.3 & -0.4\\ -1.5 & -1.5 & 0.3 & -0.4\\ -1 & -1 & 0 & 0\\ 0 & 0 & 0 & 0\end{bmatrix}, B_1 = \begin{bmatrix}-5\\ -5\\ 0\\ 0\end{bmatrix},$$
$$A_2 = \begin{bmatrix}-1.95 & -2.09 & 1.61 & 0\\ 1.59 & 1.45 & 1.21 & 0\\ 0 & 0 & -1 & 0\\ 1 & 1 & 0 & 1\end{bmatrix}, B_2 = \begin{bmatrix}10\\ 10\\ 0\\ 0\end{bmatrix},$$
$$A_3 = \begin{bmatrix}-0.78 & -0.92 & 0 & 4.34\\ -0.076 & -0.22 & 0 & -4.14\\ 0 & 0 & 1 & 0\\ -1 & -1 & 0 & -10\end{bmatrix}, B_3 = \begin{bmatrix}-10\\ -10\\ 0\\ 0\end{bmatrix},$$
$$C = \begin{bmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\end{bmatrix}^\top, D = \begin{bmatrix}1 & 1 & 0 & 0\end{bmatrix}^\top, E = \begin{bmatrix}1\\ 1\end{bmatrix}.$$

In this example, $x \in \mathbb{R}^4$ is the state, $y \in \mathbb{R}^2$ is the output, $u = 1.5$ is the known input, $d(t) = \sin(5t)$ is the unknown disturbance and $\omega(t) = \cos(2\pi(0.05t + 0.05)t)$ is a linear chirp signal. Suppose the sampling time is $\delta = 0.01$ s, and the DoS attacks are given with $\tau_{\min} = 0.5$ s and $\tau_{\max} = 0.2$ s. The system initial conditions are set as $x(0) = [4\ -3\ 2\ -2.5]^\top$. The switching law is set as

$$\sigma(t) = \begin{cases}1,\ \text{if } 2j \leq t \leq 2j+1,\ j = 0, \cdots, 4,\\ 2,\ \text{if } 4j+1 \leq t \leq 4j+2,\ j = 0, \cdots, 2,\\ 3,\ \text{if } 4j+3 \leq t \leq 4j+3,\ j = 0, 1.\end{cases}$$

Select the non-singular state transformation as

$$T = \begin{bmatrix} -0.707 & 0.707 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0.5 & 0.5 & 0 & 0 \end{bmatrix}, \; U = \begin{bmatrix} -0.707 & 0.707 \\ 0.5 & 0.5 \end{bmatrix},$$

and the partly observable transformed matrices

$$Z_1^k = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^\top, Z_2^k = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}^\top, Z_3^k = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}^\top.$$

The parameters of observers (6) and (15) are selected as $k_1 = 10$, $k_2 = 100$, $k_3 = 5$, $k_4 = 50$.

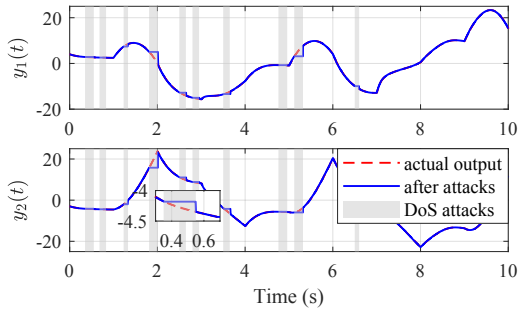

Fig. 2. Measurement y and its value after DoS attacks.

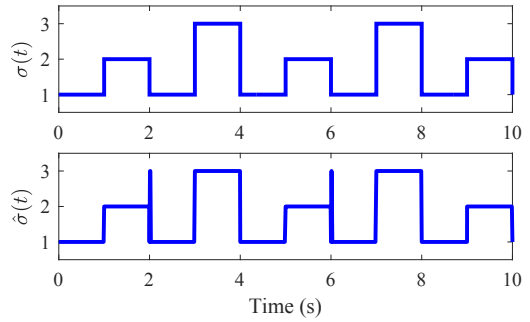

Fig. 3. Switching law σ and its estimate $\hat{\sigma}$.

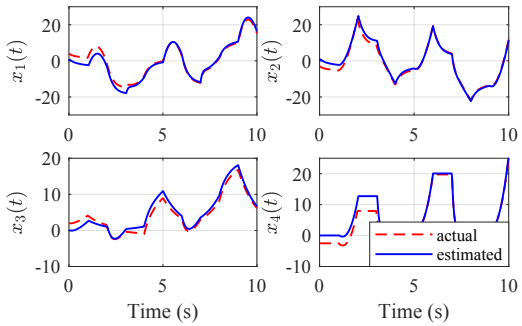

Fig. 4. State x and its estimate $\hat{x}$.

Figure 2 depicts the measured output and the output post-DoS attacks, with the gray shaded area denoting DoS attack times. Post-attack, the measured output remains constant for a period starting from the attack onset. Figure 3 shows the estimation response curve of discrete states, revealing a brief estimation error at the switching moment but quickly identifying the true switching law. Figure 4 depicts the estimation response curve for continuous states. After 4 switches (at 4 s), the observer's output accurately estimates the true system state. These results validate the effectiveness and the accuracy of our approach.

VI. Conclusion

This paper investigates secure state estimation in NSSs under noise, disturbances, and suitably bounded DoS attacks. Leveraging a high-order sliding mode approach, we develop discrete and continuous state observers enabling active mode identification and continuous state estimation. The proposed method ensures accurate estimation within finite time, accommodating DoS attacks with bounded frequency and duration characteristics without constraints on the timing or order of switching laws.

References

[1] Tipsuwan, Y., and Chow, M. Y. "Control methodologies in networked control systems." *Control Eng. Pract.*, 11(10): 1099-1111, 2003.

[2] Wang, F. Y., and Liu, D. *Networked control systems* (pp. 153-196). London: Springer, 2008.

[3] Teixeira, A., Sandberg, H., and Johansson, K. H. "Networked control systems under cyber attacks with applications to power networks." in *2010 Am. Control Conf.*, 2010: 3690-3696.

[4] Eliades, D. G., Vrachimis, S. G., Moghaddam, A., Tzortzis, I., and Polycarpou, M. M. "Contamination event diagnosis in drinking water networks: A review." *Annu. Rev. Control*, 55: 420-441, 2023.

[5] Stojkoska, B. L. R., and Trivodaliev, K. V. "A review of Internet of Things for smart home: Challenges and solutions." *J. Clean. Prod.*, 140: 1454-1464, 2017.

[6] Liberzon, D. *Switching in systems and control*, vol. 190. Boston: Birkhauser, 2003.

[7] Yang H., Jiang, B., and Cocquempot V. *Stabilization of switched nonlinear systems with unstable modes*, Switzerland: Springer, 2014.

[8] Ma, D., and Zhao, J. "Stabilization of networked switched linear systems: An asynchronous switching delay system approach." *Syst. Control Lett.*, 77: 46-54, 2015.

[9] Fu, J., Qi, Y., Xing, N., and Li, Y. "A new switching law for event-triggered switched systems under DoS attacks." *Automatica*, 142: 110373, 2022.

[10] Ding, D., Han, Q. L., Ge, X., and Wang, J. "Secure state estimation and control of cyber-physical systems: A survey." *IEEE Trans. Syst. Man Cybern. Syst.*, 51(1): 176-190, 2020.

[11] Sánchez, H. S., Rotondo, D., Escobet, T., Puig, V., and Quevedo, J. "Bibliographical review on cyber attacks from a control oriented perspective." *Annu. Rev. Control*, 48: 103-128, 2019.

[12] Ding, K., Li, Y., Quevedo, D. E., Dey, S., and Shi, L. "A multi-channel transmission schedule for remote state estimation under DoS attacks." *Automatica*, 78: 194-201, 2017.

[13] Yan, J. J., and Yang, G. H. "Secure state estimation with switched compensation mechanism against DoS attacks." *IEEE Trans. Cybern.*, 52(9): 9609-9620, 2021.

[14] Zhang, Y., Wang, Z., Zou, L., Dong, H., and Yi, X. "Neural-network-based secure state estimation under energy-constrained denial-of-service attacks: An encoding-decoding scheme." *IEEE Trans. Netw. Sci. Eng.*, 10(4): 2002-2015, 2023.

[15] Hespanha, J. P., and Morse, A. S. "Stability of switched systems with average dwell-time." in *38th IEEE Conf. Decis. Control*, 1999: 2655-2660.

[16] Spurgeon, S. K. "Sliding mode observers: a survey." *Int. J. Syst. Sci.*, 39(8): 751-764, 2008.

[17] Alessandri, A., Baglietto, M., and Battistelli, G. "Moving-horizon state estimation for nonlinear discrete-time systems: New stability results and approximation schemes," *Automatica*, 44(7): 1753-1765, 2008.

[18] De Persis, C., and Tesi, P. "Input-to-state stabilizing control under denial-of-service." *IEEE Trans. Autom. Control*, 60(11): 2930-2944, 2015.

[19] Moreno, J. A., and Osorio, M. "Strict Lyapunov functions for the super-twisting algorithm." *IEEE Trans. Autom. Control*, 57(4): 1035-1040, 2012.

[20] Tanwani, A., Shim, H., and Liberzon, D. "Observability for switched linear systems: characterization and observer design." *IEEE Trans. Autom. Control*, 58(4): 891-904, 2012.