ORIGINAL ARTICLE
Journal Section

Extended Observer-Based Hybrid Tracking Control Strategy for Networked System with FDI Attacks

Longyu Xu[1,3] | **Yong Chen**[1,2,3] | **Meng Li**[1,3] | **Longjie Zhang**[1,3] | **Gafary Mahmoud**[1,3]

[1]School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731,China

[2]Yangtze Delta Region Institute (Huzhou), University of Electronic Science and Technology of China, Huzhou 313001, China.

[3]Institute of Electric Vehicle Driving System and Safety Technology, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731,China

Correspondence
Yong Chen, School of Automation Engineering, University of Electronic Science and Technology of China, Chengdu, Sichuan 611731, China
Email: ychencd@uestc.edu.cn

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 61973331.

This paper studies the speed tracking control of networked control systems (NCSs) with external disturbance and false data injection (FDI) attacks. Firstly, the system model with external disturbances and FDI attacks is built. Then, an extended observer based on discrete time sliding function and neural network (NN) is proposed to observe the extended states and suppress the effect of external disturbance and FDI attacks. Furthermore, a novel hybrid discrete-time sliding mode control (HDSMC) strategy combining discrete time sliding mode control with super-twisting control is designed to perform closed-loop control of the system. In which, the exponential term and nonlinear term are constructed to restrain the jitters. The convergence and reachability of the sliding motion are proofed. Finally, the validity and feasibility of the proposed methods are proved by simulations and experiments.

KEYWORDS
NCSs, tracking control, FDI attacks, extended observer, and HDSMC.

1 | INTRODUCTION

NCSs are distributed control systems, whose components, including controllers, actuators, sensors, are scattered in different parts of the network. The components constitute closed-loop systems via network communication [1]. With the rapid development of network technology and computer technology, NCSs have aroused wide attention and

have been applied in many fields such as DC motor control [2], networked-vehicle [3], spaceflight [4], etc. Compared to traditional field bus control systems, NCSs have diverse advantages in terms of less wiring, easy to extend, not limited by distances, and so on. However, the introduction of the communication network results in the NCSs highly vulnerable to various network attacks. With the frequent occurrence of industrial network attacks, network security has become a key issue in network security, which has aroused wide concern [5].

There exist two main forms of attack: Denial -of Service attacks [6], and injection attacks [7], which will generate the harmful signal for the network channels. In this paper, we are concentrated on the security tracking control of NCSs under the FDI attacks, which have been studied by many researchers. In [7], to obtain the information of the FDI attacks, a novel abnormal intrusion estimator for the attacks based on NN is proposed,and the delay and packet loss are damped effectively. Furthermore, for NCSs under the stealthy FDI attacks, Mao et al. in [8] used the characterized detectability conditions to detect and observe the attacks effectively. Inspired by this work, we apply NN in observer design to estimate the FDI attacks and compensate for the attacks. Based on the observed system information, Gao et al. studied the problem of alarm response of cyber-physical systems with FDI attacks in [9]. The size of transmitted packages needs to be reduced due to the bandwidth of the communication networks. An optimal weighting fusion criterion is designed by establishing convex optimization problems to lessen the quantization errors. In [10], for the speed tracking control of networked systems under FDI attacks, a networked predictive control method based on a Kalman filter is proposed to predict and detect the attacks to weaken the attack effects. Based on a NN observer, [11] proposed a resilient control to compensate the influence of the FDI attack for the Networked smart grid systems. Compare with the linear quadratic control method, the resilient control had improved performance in the tracking control experiments. Furthermore, In [12], to analyze the influence of the FDI attacks for the tracking control, Pang, et al. studied the optimal design of the FDI attacks for the NCSs, which can show us how the FDI attacks destroy the tracking performance of the control systems. The above literature mainly analyzed the aspects of invasion estimation and interference prediction. However, researches in effective control methods of NCSs with attacks are still inadequate. As the results shown in [12], the jitters caused by FDI attacks are worrying and they will destroy the stability of the NCSs, which remain challenging and need further research.

Sliding mode control (SMC) is a significant methodology for nonlinear control has positive impact on the improvement of robustness [13]. SMC has a simple structure but responds fast and can overcome uncertainties [14]. To reduce jitters and improve control precision, many different types of SMC methods have been studied [15][16][17][18]. In [19], for the problems of unknown parameters, model uncertainly, and external disturbance, a robust adaptive nonsingular terminal sliding mode control method is proposed. In [20], a discrete-time fractional-order terminal sliding mode control method is presented for linear motor, which can maintain high-precision tracking control. Xu et al. in [21] proposed an SMC strategy based on terminal sliding mode surface, which designs a new second-order discrete-time SMC strategy for precision motion control of piezoelectrically driven Nano-positioning devices. This strategy is easy to realize and eliminates the use of state observers by using the feedback of output value. In [22], a discrete-time reaching law-based sliding mode control method is shown to effectively control the disturbed discrete-time system. Liu et al. in [23] proposed an adaptive fractional sliding mode control method based on radial basis function NN, which can online update to approximate the nonlinear system. Though there have been many previous research results, some problems still need to be further studied. For example, there are few kinds of research on using neural networks in discrete systems. The application of sliding mode control to networked systems with network problems is inadequate Also, the hybrid sliding mode control strategy combining different control methods is not enough researched.

Motivated by the abovementioned researches, the main work in this paper can be summarized: (i) according to the modeled NCSs with external disturbance and FDI attacks, an extended functional observer based on sliding mode and radial basis function neural network is proposed to suppress the errors of system states which are induced by external

disturbance and FDI attacks. Differently, the neural network is applied to estimate the attacks and compensate for the attacks. (ii) Then, a hybrid discrete-time control strategy is designed, which combines the super-twisting algorithm with discrete-time sliding mode control. Different from the traditional algorithm, the sliding surface and reaching law are designed, in which nonlinear term and exponential term are introduced to optimize the jitter suppression effect. The convergence and reachability of sliding motion are proved subsequently. Finally, the effectiveness of the proposed method is illustrated through simulations and experiments. The rest of this paper is constructed as follows. In section 2, the system with external disturbance and attacks is modeled. The extended functional observer is designed and proved in section 3. Then, in section 4, the HDSMC method is designed to improve the control effectiveness. The convergence and reachability are also analyzed. Section 5 shows the simulation and experiment results. Finally, conclusions are summarized in section 6.

2 | PROBLEM DESCRIPTION

In this part, the networked system is modeled. In this model, due to signal interference or other external disturbances, the systems usually gets disturbed. Also, the output signal of the sensors delivered to the controller is transmitted via the network, where the attacker attempts to use the FDI attack to inject false data into the transmitted data, which will also be affected by the network noises and make the signal different from the original. In which case, if without an appropriate suppression strategy, the system may become unstable.

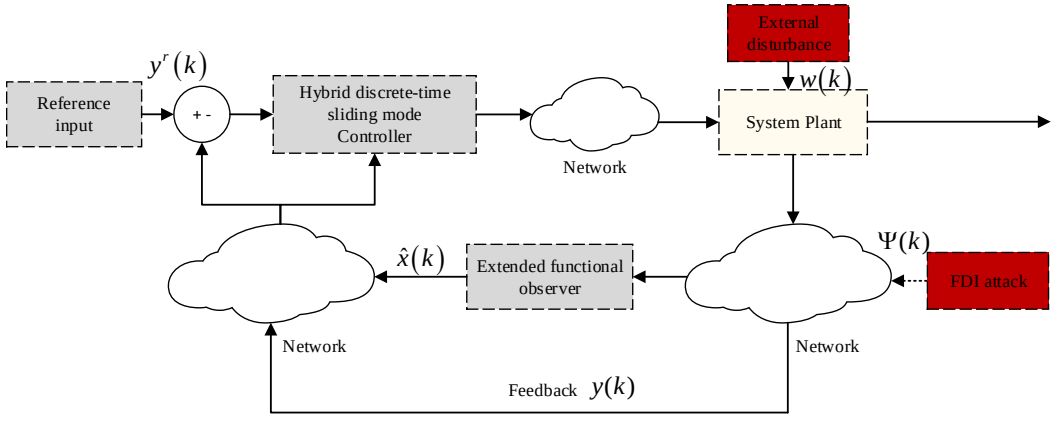

FIGURE 1 Networked control system with external disturbance and FDI attack

Based on the above, consider the networked system with FDI attack and external disturbance as follow, the structure is shown in FIGURE 1.

$$x(k+1) = Gx(k) + Hu(k) + w(k) \tag{1}$$

$$y(k) = Cx(k) + \Psi(k) \tag{2}$$

where k represents the discrete-time index, $x(k) = [x_1(k), x_2(k), \dots, x_n(k)]^T$, $u(k)$ are the state and control input. $w(k) = [w_1(k), w_2(k), \dots, w_n(k)]^T$ is disturbance introduced by network or system parameter drift, which satisfies

the energy constraint $\|w(k)\|_2 \leq W$. $\Psi(k)$is the and measurement channel noise function. The attacker launches FDI attacks with limited energy $\|\Psi(k)\|_2 \leq \psi$, $\|\Psi(k) - \Psi(k-1)\|_2 \leq \Psi_d$ for the output signal $y(k)$ to offset the right signal.

Remark 1: Here, we mainly concentrate on the false data injection on the sensor measurement channels. For the simplification of the control design, the other interferences should be simplified or merged. As shown in (1), the external disturbances considered in this paper are the system disturbances, which are generated by the network noises in actuator communication channels and system operating environment noises. As the work described in [24] and [25], the system disturbances can be regarded as the unknown input. In our work, we concentrate on the network channel noises, which will be input through the control input channels and the corresponding function can be expressed as $Hw_n(k)$. The other system noises come from the external environment can be expressed as $H^r w_e(k)$. Then, we can get the general model of the system $w(k) = Hw_n(k) + H^r w_e(k)$ for the convenience of the controller design. The false data injection attacks will violate data integrity through modifying data packets [26]. For the observer/estimator-based control system, the attackers can inject the false data into the measurement channels, which will cause negative impact on the accuracy of the observer/estimator [27]. Considering the above problems, we mainly concentrate on the resistance of the attacks on sensor channels and improve the observer-based control performance. Moreover, there will exist network noises in the sensor measurement channels, which can be expressed as $d(t)$ and the attacks are $\Psi_s(k)$. In this paper, because the disturbances and attacks both exist in the sensor channels at the same time, we regard them as the malicious unknown inputs $\Psi(k) = d(t) + \Psi_s(k)$ and avoid dealing with these two problem separately.

3 | ATTACK AND DISTURBANCE SUPPRESSION DESIGN

In this part, a discrete-time extended functional observer combining SMC with radial basis function (RBF) NN is designed to effectively reduce the influence of FDI attack and external disturbance. And the convergence is analyzed.

3.1 | Design of Extended Functional Observer

Let $\bar{x}(k) = [x(k), \Psi(k)]^T$, $\bar{E} = [I_n, 0_{n\times p}]$, $\bar{G} = [G, 0_{n\times p}]$ and $\bar{C} = [C, I_p]$. So, the system can be redesigned as follows

$$\begin{cases} \bar{E}\bar{x}(k+1) = \bar{G}\bar{x}(k) + Hu(k) + w(k) \\ y(k) = \bar{C}\bar{x}(k) \end{cases} \tag{3}$$

Design an extended functional observer as following [14]:

$$\begin{cases} \wp(k+1) = M\wp(k) + Ny(k) + Fu(k) + v(k) \\ \hat{\bar{x}}(k) = \wp(k) + Jy(k) \end{cases} \tag{4}$$

in which, $\wp(k)$ is a temporary value introduced in to help estimate the extended system states. $\hat{\bar{x}}(k)$ represents the estimated value of $\bar{x}(k)$. Matrices M,N,F,J denote the observer parameters. $v(k)$ here is used to compensate for the external disturbance. Define $R = \begin{bmatrix} I_n \\ -C \end{bmatrix}$,$S = \begin{bmatrix} 0_{n\times p} \\ I_p \end{bmatrix}$, assume that the pair $(R\bar{G}, \bar{C})$is observable.

Theorem 1: For the system mentioned in (3), along with the observer proposed in (4), if $w(k) = 0$ and the pair $(R\bar{G}, \bar{C})$is obervable, the estimation error $\bar{e}(k) = \hat{\bar{x}}(k) - \bar{x}(k)$ will converge to zero.

The parameters of the observer can be calculated as:

$$M = R\bar{G} - Z\bar{C} \tag{5}$$

where Z is a gain matrix.

Proof: To make the analysis process easier without losing the truth, we let $w(k) = 0$ as [14], multiply R to the first equation of (3) equals:

$$R\bar{E}\bar{x}(k+1) = R\bar{G}\bar{x}(k) + RHu(k) \tag{6}$$

Add $Sy\,(k+1)$ to (6), according to the second equation of (3), (6) can be written as:

$$S\bar{C}\bar{x}\,(k+1) + R\bar{E}\bar{x}\,(k+1) = R\bar{G}\bar{x}(k) + RHu(k) + Sy\,(k+1) \tag{7}$$

Notice that $S\bar{C} + R\bar{E} = I_{n+q}$. Hence (7) equals

$$\bar{x}\,(k+1) = R\bar{G}\bar{x}(k) + RHu(k) + Sy\,(k+1) \tag{8}$$

Define $\Lambda\,(k) = RHu(k) + Sy\,(k+1)$, system (3) can be represented as

$$\begin{cases} \bar{x}\,(k+1) = R\bar{G}\bar{x}(k) + \Lambda\,(k) \\ y\,(k) = \bar{C}\bar{x}\,(k) \end{cases} \tag{9}$$

Hence, the observer can be designed as

$$\hat{\bar{x}}\,(k+1) = R\bar{G}\hat{\bar{x}}(k) + \Lambda\,(k) + Z\left(y\,(k) - \bar{C}\hat{\bar{x}}\,(k)\right) \tag{10}$$

Define $\wp\,(k) = \hat{\bar{x}}(k) - Sy\,(k)$, so that

$$\begin{aligned} &\wp\,(k+1) = \hat{\bar{x}}(k+1) - Sy\,(k+1) \\ &= R\bar{G}\hat{\bar{x}}(k) + \Lambda\,(k) + Z\left(y\,(k) - \bar{C}\hat{\bar{x}}\,(k)\right) - Sy\,(k+1) \\ &= R\bar{G}\hat{\bar{x}}(k) + RHu(k) + Sy\,(k+1) + Z\left(y\,(k) - \bar{C}\hat{\bar{x}}\,(k)\right) - Sy\,(k+1) \\ &= R\bar{G}\hat{\bar{x}}(k) + RHu(k) + Z\left(y\,(k) - \bar{C}\hat{\bar{x}}\,(k)\right) \\ &= \left(R\bar{G} - Z\bar{C}\right)\hat{\bar{x}}(k) + RHu(k) + Zy\,(k) \\ &= \left(R\bar{G} - Z\bar{C}\right)(\wp\,(k) + Sy\,(k)) + RHu(k) + Zy\,(k) \\ &= \left(R\bar{G} - Z\bar{C}\right)\wp\,(k) + \left(R\bar{G} - Z\bar{C}\right)Sy\,(k) + RHu(k) + Zy\,(k) \\ &= \left(R\bar{G} - Z\bar{C}\right)\wp\,(k) + RHu(k) + \left[\left(R\bar{G} - Z\bar{C}\right)S + Z\right]y\,(k) \end{aligned} \tag{11}$$

Combining (11) with the observer (11), the parameters of the observer can be calculated as (5). This completes the proof.

3.2 | The NN observer design and convergence analysis

Define the observer error as follow

$$\bar{e}(k) = \hat{\bar{x}}(k) - \bar{x}(k) \tag{12}$$

According to (8), (10), (12), $\bar{e}(k+1)$ equals:

$$\begin{aligned}
&\bar{e}(k+1) = \hat{\bar{x}}(k+1) - \bar{x}(k+1) \\
&= R\bar{G}\hat{\bar{x}}(k) + \Lambda(k) + Z\left(y(k) - \bar{C}\hat{\bar{x}}(k)\right) \\
&-R\bar{G}\bar{x}(k) - RHu(k) - Sy(k+1) \\
&= R\bar{G}\hat{\bar{x}}(k) + RHu(k) + Sy(k+1) + Z\left(y(k) - \bar{C}\hat{\bar{x}}(k)\right) \\
&-R\bar{G}\bar{x}(k) - RHu(k) - Sy(k+1) \\
&= R\bar{G}\hat{\bar{x}}(k) - R\bar{G}\bar{x}(k) + Z\left(y(k) - \bar{C}\hat{\bar{x}}(k)\right) \\
&= \left(R\bar{G} - Z\bar{C}\right)\bar{e}(k)
\end{aligned} \tag{13}$$

Define $\Delta\bar{e}(k) = \bar{e}(k) - \bar{e}(k-1)$, and introduce the sliding function as follow:

$$s(k) = q_1\bar{e}(k) + q_2\Delta\bar{e}(k) \tag{14}$$

where $q_1 > 0$, $q_2 > 0$ are the corresponding parameters. Design the sliding mode control input as follow:

$$u_s(k) = \mu sign(s(k)) \cdot |s(k)|^{1/2} \tag{15}$$

where $\mu > 0$ is the control parameter, $sign(f(k))$ represents the sign of function $f(k)$.

The sliding mode control law can be defined as:

$$v(k) = \lambda_1 u_s(k) + \lambda_2 u_n(k) \tag{16}$$

where the term $u_n(k)$is an adaptive compensation derivate from NN. $\lambda_1 > 0$ and$\lambda_2 > 0$ are the weight parameters, which satisfy $\lambda_1 + \lambda_2 = 1$.

The RBF NN is used to approximate the desired bound of the system uncertainties as:

$$\hat{\bar{\Phi}}(\hat{x}, \hat{W}) = \hat{W}^T\varphi(\hat{x}) \tag{17}$$

where $\hat{x}$ is the input of the RBF NN, $\hat{W} \in R^n$is the weight vector of the RBF NN, n is the number of nodes in the hidden layer, and the vector $\varphi(\hat{x}) \in R^n$ is Gaussian type of functions defined element-wise as:

$$\varphi_i(\hat{x}) = \exp(-(\hat{x} - c_i)^T(\hat{x} - c_i)\Big/\sigma_i^2), i = 1, \cdots, n \tag{18}$$

where $c_i \in R^{m\times n}$ and $\sigma_i \in R^n$denote the center and width of the ith hidden node respectively and they are predetermined by using the local training method [28].

There exists an arbitrary positive constant ζ_0, an optimal constant weight vector W^* such that the output of the

optimal RBF NN with enough hidden nodes satisfies:

$$W^{*}\varphi(\hat{x}) - \bar{\Phi}(k) = \zeta_{f} < \zeta_{0} \tag{19}$$

where ζ_f denotes the error between the desired upper bound and the estimated upper bound obtained from RBF NN.

To design the RBF NN-based DSMO, the adjustment of the weight vector and the analysis of the estimation error convergence, the input of the DSMO can be designed as below.

Supposing the ideal input of $u_n(k)$ as $u_n^*(k)$, $u_n^*(k)$ satisfies the following formulation:

$$u_n^*(k) = W^{*T} h(z) + \varepsilon(z) \tag{20}$$

There exists positive constant W_m and ε_m such that the optimal constant weight vector W^* and the approximate error satisfies:

$$\|W^{*}\| \leq W_m, |\varepsilon(z)| \leq \varepsilon_m \tag{21}$$

Define the actual NN weight as $\hat{W}(k)$, so that the control law designed by RBF NN is shown as follow

$$u_n(k) = \hat{W}^{T}(k) h(z) \tag{22}$$

where $h(z)$ is the output value of Gaussian type of function, $z \triangleq \bar{x}(k)$ is the input value of RBF NN.

According to (22), the following conclusion can be obtained:

$$u_n(k) - u_n^*(k) = \hat{W}^{T}(k) h(z) - W^{*T} h(z) - \varepsilon(z) \tag{23}$$

Define $\tilde{W} = W^{*} - \hat{W}$ so that

$$u_n(k) - u_n^*(k) = \tilde{W}^{T}(k) h(z) - \varepsilon(z) \tag{24}$$

Select the weight update algorithm as follow:

$$\tilde{W}(k+1) = \tilde{W}(k) - \eta\left(h(z)\,\bar{e}(k+1) + \vartheta\hat{W}(k)\right) \tag{25}$$

where η and ϑ are positive. Based on above, (25) can be derivate as

$$\hat{W}(k+1) = \hat{W}(k) - \eta\left(h(z)\,\bar{e}(k+1) + \vartheta\hat{W}(k)\right) \tag{26}$$

According to (16), (20), (22)

$$\tilde{W}^{T}(k) h(z) = \bar{e}(k+1) + \varepsilon(z) \tag{27}$$

From the observer designed, the estimated states $\hat{x}(k)$ and estimated FDI attack $\hat{\psi}(k)$ can be obtained.

$$\hat{\bar{x}}(k+1) = \left(I - J\bar{C}\right)^{-1}\left\{\left[M + (N - MJ)\,\bar{C}\right]\hat{\bar{x}}(k) + Fu(k) + v(k)\right\} \tag{28}$$

Define the matrices as follow to simplify the equation: $\Theta_1 = \left(I - J\bar{C}\right)^{-1}\left[M + (N - MJ)\,\bar{C}\right]$, $\Theta_2 = \left(I - J\bar{C}\right)^{-1}F$, $\Theta_3 = \left(I - J\bar{C}\right)^{-1}$. Since $\hat{\bar{x}}(k) = \begin{bmatrix} \hat{x}(k) \\ \hat{\psi}(k) \end{bmatrix}$, the extended system can be reshaped as:

$$\begin{bmatrix} \hat{x}(k+1) \\ \hat{\psi}(k+1) \end{bmatrix} = \begin{bmatrix} \Theta_{11}, \Theta_{12} \\ \Theta_{13}, \Theta_{14} \end{bmatrix}\begin{bmatrix} \hat{x}(k) \\ \hat{\psi}(k) \end{bmatrix} + \begin{bmatrix} \Theta_{21} \\ \Theta_{22} \end{bmatrix}u(k) + \begin{bmatrix} \Theta_{31} \\ \Theta_{32} \end{bmatrix}v(k) \tag{29}$$

Hence, the original state can be written as:

$$\hat{x}(k+1) = \Theta_{11}\hat{x}(k) + \Theta_{12}\hat{\psi}(k) + \Theta_{21}u(k) + \Theta_{31}v(k) \tag{30}$$

Remark 2: In this part, a novel observer is designed based on the sliding mode theory and neural networks. Through the RBF NN (17), the uncertainties information that include attacks and disturbances can be obtained and compensated. The design of the adaptive law (25) and sliding mode control law (15) make the stability of the systems. In the next part, the convergence of the observation errors and unknown parameter estimation errors will be analyzed.

Theorem 2: By implementing the NN obsever (30) with adaptive law (26), the observer error (12) and weight estimation error $\bar{W}$ will be convergent with the parameters which satisfy:

$$\begin{cases} g \geq 1 \\ 0 < \eta\,(1 + \vartheta)\,l \leq 1 - \frac{1}{g} \\ 0 < \eta\,(l + \vartheta) \leq 1 \end{cases} \tag{31}$$

Proof: The Lyapunov function is considered as follow:

$$V(k) = \bar{e}^2(k) + \frac{1}{\eta}\tilde{W}^T(k)\,\tilde{W}(k) \tag{32}$$

Thus, $\Delta V(k) \triangleq V(k+1) - V(k)$ equals:

$$\begin{aligned} &\Delta V(k) = \bar{e}^2(k+1) - \bar{e}^2(k) + \tfrac{1}{\eta}\left(\tilde{W}^T(k+1)\,\tilde{W}(k+1) - \tilde{W}^T(k)\,\tilde{W}(k)\right) \\ &= \bar{e}^2(k+1) - \bar{e}^2(k) + \tfrac{1}{\eta}\left[\tilde{W}(k) - \eta\left(h(z)\,\bar{e}(k+1) + \vartheta\hat{W}(k)\right)\right]^T \times \\ &\left[\tilde{W}(k) - \eta\left(h(z)\,\bar{e}(k+1) + \vartheta\hat{W}(k)\right)\right] - \tfrac{1}{\eta}\tilde{W}^T(k)\,\tilde{W}(k) \\ &= \bar{e}^2(k+1) - \bar{e}^2(k) - 2\tilde{W}^T(k)\,h(z)\,\bar{e}(k+1) \\ &-2\vartheta\tilde{W}^T(k)\,\hat{W}(k) + \eta h^T(z)\,h(z)\,\bar{e}^2(k+1) \\ &+2\eta\vartheta\hat{W}^T(k)\,h(z)\,\bar{e}(k+1) + \eta\vartheta^2\hat{W}^T(k)\,\hat{W}(k) \end{aligned} \tag{33}$$

in which, $|h_i(z)| \leq 1, \|h(z)\| \leq l^{1/2} \leq l, h^T(z)\,h(z) = \|h(z)\|^2 \leq l, i = 1, 2, \ldots, l$.

So that following conclusion can be obtained:

$$\begin{aligned}
&2\vartheta\tilde{W}^T(k)\hat{W}(k)\\
&=\vartheta\tilde{W}^T(k)\left(\tilde{W}(k)-W^*\right)+\vartheta\left(\hat{W}(k)-W^*\right)^T\hat{W}(k)\\
&=\vartheta\left(\left\|\tilde{W}(k)\right\|^2+\left\|\hat{W}(k)\right\|^2+\tilde{W}^T(k)W^*-W^*\hat{W}(k)\right)\\
&=\vartheta\left(\left\|\tilde{W}(k)\right\|^2+\left\|\hat{W}(k)\right\|^2-\|W^*\|^2\right)
\end{aligned} \tag{34}$$

$$\eta h^T(z)h(z)\bar{e}^2(k+1)\le\eta l\bar{e}^2(k+1) \tag{35}$$

$$2\eta\vartheta\hat{W}^T(k)h(z)\bar{e}(k+1)\le\eta\vartheta l\left[\left\|\hat{W}(k)\right\|^2+\bar{e}^2(k+1)\right] \tag{36}$$

$$\eta\vartheta^2\hat{W}^T(k)\hat{W}(k)=\eta\vartheta^2\left\|\hat{W}(k)\right\|^2 \tag{37}$$

Based on (34)-(37), (33) can be written as:

$$\begin{aligned}
&\Delta V(k)\le\bar{e}^2(k+1)-\bar{e}^2(k)\\
&-2\tilde{W}^T(k)h(z)\bar{e}(k+1)-\vartheta\left(\left\|\tilde{W}(k)\right\|^2+\left\|\hat{W}(k)\right\|^2-\|W^*\|^2\right)\\
&+\eta l\bar{e}^2(k+1)+\eta\vartheta l\left[\left\|\hat{W}(k)\right\|^2+\bar{e}^2(k+1)\right]+\eta\vartheta^2\left\|\hat{W}(k)\right\|^2\\
&=(-1+\eta(1+\vartheta)l)\bar{e}^2(k+1)-\bar{e}^2(k)-2\varepsilon(z)\bar{e}(k+1)\\
&-\vartheta\left\|\tilde{W}(k)\right\|^2+\vartheta\|W^*\|^2+\vartheta(-1+\eta l+\eta\vartheta)\left\|\hat{W}(k)\right\|^2
\end{aligned} \tag{38}$$

Combining with (32), so that:

$$-2\varepsilon(z)\bar{e}(k+1)\le g\varepsilon_m^2+\frac{\bar{e}^2(k+1)}{g} \tag{39}$$

where g is a positive parameter.

Moreover,

$$\begin{aligned}
&\Delta V(k)\le\left(-1+\eta(1+\vartheta)l+\tfrac{1}{g}\right)\bar{e}^2(k+1)-\bar{e}^2(k)-\vartheta\left\|\tilde{W}(k)\right\|^2\\
&+\vartheta\|W^*\|^2+\vartheta(-1+\eta l+\eta\vartheta)\left\|\hat{W}(k)\right\|^2+\vartheta W_m^2+g\varepsilon_m^2
\end{aligned} \tag{40}$$

when the parameters in (40) satisfy:

$$\begin{cases}
g\ge 1\\
0<\eta(1+\vartheta)l\le 1-\frac{1}{g}\\
0<\eta(l+\vartheta)\le 1
\end{cases} \tag{41}$$

under this circumstance the Lyapunov function (32) will be convergent. Then the proving is finished.

4 | ROBUST TRACKING CONTROL DESIGN

In this part, a hybrid sliding mode control method based on discrete-time sliding mode control and the super-twisting algorithm is presented to furtherly improve the tracking effect and robustness.

4.1 | Design of Sliding Mode Controller

The error of output defines as follow:

$$err(k) = y^r(k) - y(k) \tag{42}$$

where $y(k)$is the actual output value of the system under FDI attack, while $y^r(k)$is the reference input.

The sliding mode function of discrete-time is designed as follow:

$$\sigma(k) = \alpha\Delta err(k) + \beta|err(k-1)|^{q/p} \cdot sign(err(k-1)) \tag{43}$$

where $\alpha > 0$,$\beta > 0$are the gain parameters. p and $q$are positive odd numbers satisfying $q/p \in (0, 1)$. And$\Delta err(k)$ is defined as $\Delta err(k) \triangleq err(k) - err(k-1)$.

Select a reaching law as follow:

$$\sigma(k+1) = \varsigma_1\sigma(k) \cdot sign(\sigma(k)) + \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(k)\right) + \varsigma_3 sign(\sigma(k)) \tag{44}$$

where $0 < \varsigma_1 < 1$,$0 < \varsigma_2 < 1$,$\varsigma_3 < 0$ are control parameters, and $sig^x(f(k)) \triangleq \|f(k)\|^x \cdot \tanh(f(k))$.

Let $\sigma(k+1) = \sigma(k)$, so that the equivalent control law can be obtained:

$$\begin{aligned} u^c_{eq}(k) = {\Theta_{21}}^{-1}\{C^{-1}[y^r(k+1) - \tfrac{1}{\alpha}(\varsigma_1\sigma(k) \cdot sign(\sigma(k)) + \\ \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(k)\right) + \varsigma_3 sign(\sigma(k)) + \beta err(k-1)^{q/p}) - err(k)] \\ -\left(\Theta_{11}\hat{x}(k) + \Theta_{12}\hat{\psi}(k) + \Theta_{31}v(k)\right)\} \end{aligned} \tag{45}$$

While the whole equivalent control law is selected as the following form:

$$u^c(k) = \lambda_3 u^c_{eq}(k) + \lambda_4 u^c_s(k) \tag{46}$$

in which $u^c_s(k)$ is the control input with the form of the super-twisting algorithm shown in (47) and (48). $\lambda_3 > 0$ and $\lambda_4 > 0$ are the weight parameters, which satisfy $\lambda_3 + \lambda_4 = 1$.

$$u^c_s(k) = -\Gamma_1|\sigma(k)|^{\frac{1}{2}} sign(\sigma(k)) + \tau(k) \tag{47}$$

$$\tau(k+1) = -\Gamma_2 sign(\sigma(k)) \tag{48}$$

where $\Gamma_1 > 0$ and $\Gamma_2 > 0$are the constant gains that need to be designed.

Remark 3: The super-twisting sliding mode function (43) can speed the convergence up. By designing a new reaching law which contains the estimation of the attacks in (44), the influence of the attack can be damped in the finite

time according to the basic principle of the sliding mode control [29]. To further promote system convergence, an equivalent control law (46) is designed with weight parameters, which can improve the convergence property of the system while ensuring the attenuation of attack influence.

4.2 | Analysis of the Sliding Motion

Definition 1: If given inequation as following is satisfied, then the sliding motion accessibility is proved [29].

$$|\sigma(k+1)| \leq |\sigma(k)| \tag{49}$$

Lemma 1: Assume that the term containing estimated FDI attack error satisfies the following condition:

$$\left\| sig^{1/2}\left(\Delta\hat{\psi}(k)\right)\right\| < \|\varsigma_3\| \tag{50}$$

Proof: From (13), the observer errors will satisfy that $\tilde{e}(k) \approx M\tilde{e}(k-1) \approx \cdots \approx M^k\tilde{e}(0)$. And because M is Hurwitz, that is $|\lambda_{\max}(M)| < 1$, then we can get that $\tilde{e}(k) \leq |\lambda_{\max}(M)|^k\tilde{e}(0) = \varepsilon(k)$, according to the definition of the error $\hat{\psi}(k) \leq \varepsilon(k) + \psi(k)$ and the boundedness of the difference of FDI attacks, the change of the attack estimation is obtained as $\left\|\Delta\hat{\psi}(k)\right\|^{1/2} \leq \|\Delta\psi(k) + \Delta\varepsilon(k)\|^{1/2} \leq \|\Delta\psi(k)\| + \|\Delta\varepsilon(k)\|^{1/2} \leq {\Psi_d}^{1/2} + d$, where $d = \|(|\lambda_{\max}(M)| - 1)\tilde{e}(0)\|^{1/2}$. If we let $\|\varsigma_3\| > {\Psi_d}^{1/2} + d$, then $sig^{1/2}(\Delta\hat{\psi}(k)) \leq \left\|\Delta\hat{\psi}(k)\right\|^{1/2} tanh(\Delta\hat{\psi}(k)) < \|\varsigma_3\|$.

Theorem 3: If the above-mentioned inequation is satisfied, for the discrete-time system in (1), the sliding mode function in (43), as well as the equivalent control law in (46), the trajectories of the system will finally arrive into the sliding mode bandwidth within finite steps.

Proof: The proof process can be separated into two steps: sliding motion accessibility and convergence in finite steps.

According to (50), the sliding motion accessibility can be formulated as:

$$\begin{aligned}&\sigma(k+1) - \sigma(k)\\ &= \varsigma_1\sigma(k) \cdot sign(\sigma(k)) + \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(k)\right)\\ &+\varsigma_3 sign\left(\sigma(k)\right) - \sigma(k)\end{aligned} \tag{51}$$

When $\sigma(k) \geq 0$

$$\begin{aligned}&\sigma(k+1) - \sigma(k)\\ &= (\varsigma_1 - 1)\sigma(k) + \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(k)\right) + \varsigma_3\end{aligned} \tag{52}$$

where, according to assumption 1,equals:

$$\varsigma_2\left\| sig^{1/2}\left(\Delta\hat{\psi}(k)\right)\right\| + \varsigma_3 < \varsigma_2\|\varsigma_3\| + \varsigma_3 \tag{53}$$

Combining with $0 < \varsigma_1, \varsigma_2 < 1, \varsigma_3 < 0$ and (53), it can be calculated that $\sigma(k+1) - \sigma(k) \leq 0$. When $\sigma(k) \leq 0$, the same conclusion can be derived. So that (49) is satisfied. From the above proof steps, the sliding motion accessibility has been proofed.

When $\sigma(k) \geq 0$, assume that the sliding motion will not cross the sliding surface when approaching the stable state.

$$\sigma(1) = \varsigma_1\sigma(0) + sig^{1/2}\left(\Delta\hat{\psi}(0)\right) + \varsigma_3 \tag{54}$$

where $sig^{1/2}\left(\Delta\hat{\psi}(0)\right)$ contains the estimation attack error at the initial time, which can be regarded as zero.

$$\begin{aligned}
&\sigma(2)\\
&= \varsigma_1\sigma(1) + \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(1)\right) + \varsigma_3\\
&= \varsigma_1\left(\varsigma_1\sigma(0) + \varsigma_3\right) + \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(1)\right) + \varsigma_3\\
&= \varsigma_1^2\sigma(0) + \varsigma_1\varsigma_3 + \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(1)\right) + \varsigma_3
\end{aligned} \tag{55}$$

.....

$$\begin{aligned}
&\sigma(i)\\
&= \varsigma_1\sigma(i-1) + \varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(i-1)\right) + \varsigma_3\\
&= \varsigma_1^i\sigma(0) + \varsigma_1^{i-1}\varsigma_3 + \varsigma_1^{i-2}\varsigma_3 + \ldots + \varsigma_1^0\varsigma_3\\
&+ \varsigma_1^{i-2}\varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(1)\right) + \varsigma_1^{i-3}\varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(2)\right)\\
&+ \ldots + \varsigma_1^0\varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(i-1)\right)
\end{aligned} \tag{56}$$

According to assumption 1, $\sigma(i)$ can be zoomed into:

$$\begin{aligned}
&\sigma(i)\\
&= \varsigma_1^i\sigma(0) + \varsigma_1^{i-1}\varsigma_3 + \varsigma_1^{i-2}\varsigma_3 + \ldots + \varsigma_1^0\varsigma_3\\
&+ \varsigma_1^{i-2}\varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(1)\right) + \varsigma_1^{i-3}\varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(2)\right)\\
&+ \ldots + \varsigma_1^0\varsigma_2 sig^{1/2}\left(\Delta\hat{\psi}(i-1)\right)\\
&\leq \varsigma_1^i\sigma(0)\\
&+ \varsigma_1^{i-1}\varsigma_3 + \varsigma_1^{i-2}\varsigma_3 + \ldots + \varsigma_1^0\varsigma_3\\
&+\varsigma_1^{i-2}\varsigma_2\varsigma_3+\varsigma_1^{i-3}\varsigma_2\varsigma_3+\ldots+\varsigma_1^0\varsigma_2\varsigma_3
\end{aligned} \tag{57}$$

Let $\sigma(i)=0$, according to $0 < \varsigma_1, \varsigma_2 < 1$, $\varsigma_3 < 0$ and (50), an effective solution can be calculated. $i^* = \left\lfloor f\left(\sigma(0), \varsigma_1, \varsigma_2, \varsigma_3\right)\right\rfloor$ is the finite step. When $\sigma(k) \leq 0$, a similar conclusion can be obtained. From the above proof steps, the convergence in finite steps has been proofed. This completes the proof.

5 | SIMULATION AND EXPERIMENT RESULTS

In this section, both numerical simulation and practical experiments are carried out to show the effectiveness of the proposed control methodology.

5.1 | Numerical Simulation

In this subsection, the numerical simulation is based on the system proposed in the formulation (1), the parameters are $G = \begin{bmatrix} 0.9647 & -0.0282 \\ 0.0196 & 0.9997 \end{bmatrix}, H = \begin{bmatrix} 0.0196 \\ 0.0002 \end{bmatrix}, C = \begin{bmatrix} -0.2293 \\ 1.4393 \end{bmatrix}^T$. External disturbance $w(k) = 2\sin 3k + 3\cos 2k$. The FDI attack point is selected by random seed, and the attack size is randomly associated with the output signal. The gain of the observer is $Z = [0.07 \; -0.1042 \; 0.3736]^T$, and the corresponding parameters are as follows: $q_1 = 0.03$, $q_2 = 0.22$, $\mu = 0.06$. $\lambda_1 = 0.9$, $\lambda_2 = 0.1$. The parameters of the sliding controller are: $\alpha = 0.03$, $\beta = 5$, $q/p = 3/5$, $\varsigma_1 = 0.1$, $\varsigma_2 = 0.9$, $\varsigma_3 = -10$, $\lambda_3 = 0.65$, $\lambda_4 = 0.35$, $\Gamma_1 = 260$, $\Gamma_2 = 0.5$. All the initial values are set as zero.

The simulation results are explained as follows.

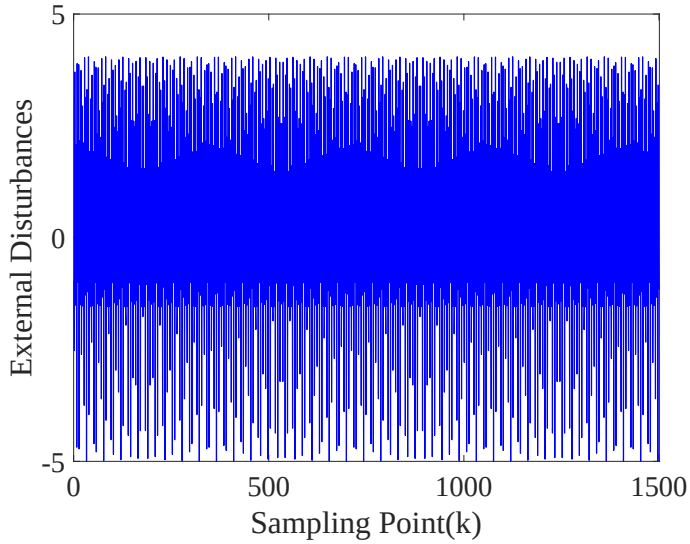

FIGURE 2 External disturbance of the system

FIGURE 2 shows the external disturbance injected into the system states, which is a mixed sinusoidal signal in general. This item is used to simulate the network interference that the system may encounter during network transmission, and it can also be replaced with other types of bounded interference with upper bound $\|w(k)\| \leq 4$.

FIGURE 3 depicts the output tracking trajectories at the speed of 1500 rad/min with random FDI attacks. The proposed control method, HDSMC, along with the discrete-time sliding mode control method, which works without the super-twisting algorithm is compared. The proposed method, at about the 66^{th} point (about 3s) begins to let the system stable. While the compared method becomes stable about 89^{th} points, which is later than proposed method for about 0.6s. Meanwhile, the compared method has more static error 32, which is larger than the proposed one 4 as shown in FIGURE 3. Moreover, when the FDI attack launches, the proposed method becomes stable again quicker than the compared one.

FIGURE 4 shows the corresponding control input of the methods. From which, it can be seen that the proposed method consumes less energy to become stable when the attack happens. FIGURE 5 reflects the sliding surface of the system via two different methods. The sliding motion of the proposed method approaches to stable state much quicker with 16 sample points than the compared one. Moreover, the proposed method gets a smaller approach error

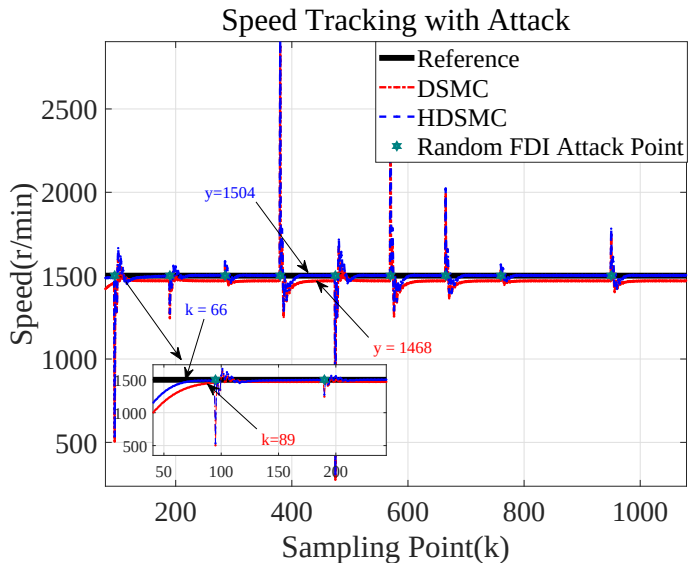

FIGURE 3 Output tracking of the system at a fixed speed

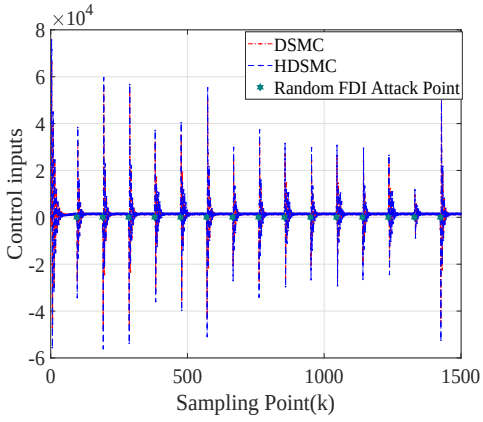

FIGURE 4 Control input of the system at a fixed speed

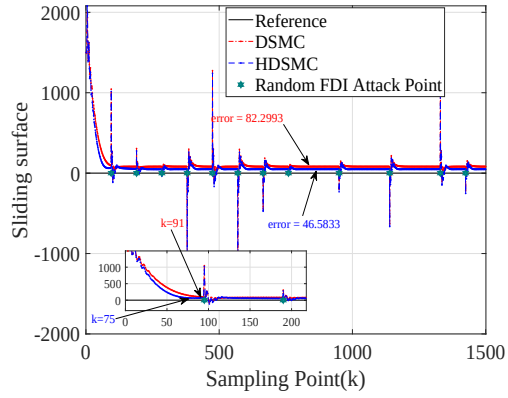

FIGURE 5 Sliding surface of the system at a fixed speed

46.5833, which is smaller than 82.2933 of DSMC.

To furtherly compare the performance of the two different methods. The simulation of tracking control with speed varying from 1500rad/min to 2500 rad/min is carried out. Results are shown in the following.

FIGURE 6 represents the output tracking trajectories of the system at changed speed with the two different control methods. The proposed controller performs better than the compare one. When speed changes, the proposed control method reacts faster with 27 sample points, and tracks more precisely, while the compared one has a significant static error. When the FDI attack launches, the proposed method jitters slighter and stabilizes rapidly.

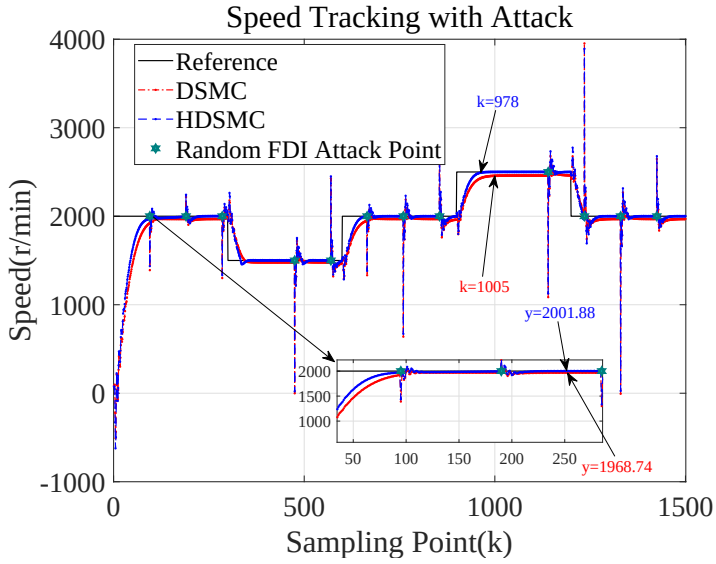

FIGURE 6 Output tracking of the system at changed speed

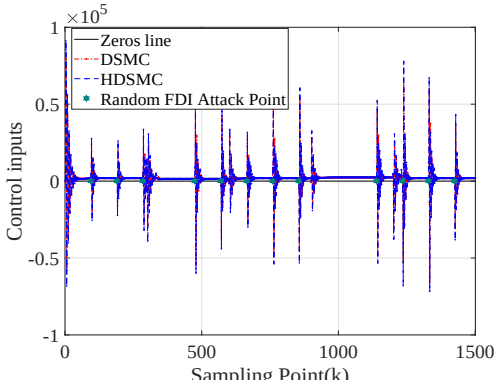

FIGURE 7 Control input of the system at changed speed

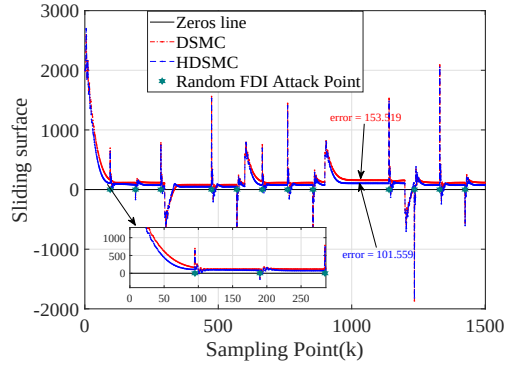

FIGURE 8 Sliding surface of the system at changed speed

Analogously, a simulation is executed to compare the control input and sliding motion performance. The results are shown in FIGURE 7 and FIGURE 8. Same as the aforementioned conclusion, the proposed method performs better in tacking response and tracking accuracy. When an attack occurs, the system deviates from a stable tracking speed.

Both methods can restore the system to stability. However, the proposed method has better advantages. From the control input diagram, the proposed method consumes less control resources. From the perspective of sliding mode motion trajectory, the proposed method can recover to a balanced state faster, and has a smaller sliding mode jitter with 101.559 bandwidth and less than the 153.519 of DSMC, thereby reducing the static jitter of the system.

5.2 | Practical Experiment

In this part, practical experiments are carried out on the NetController plant. As is shown in FIGURE 9, the plant contains a DC motor system, a NetController, and a monitoring system. Each part is connected via the network. The set model is downloaded to the controller through the PC via the network. The controller executes the corresponding program and acts on the DC motor system. The corresponding control parameters of the controller are transmitted back to the monitoring system through the network.

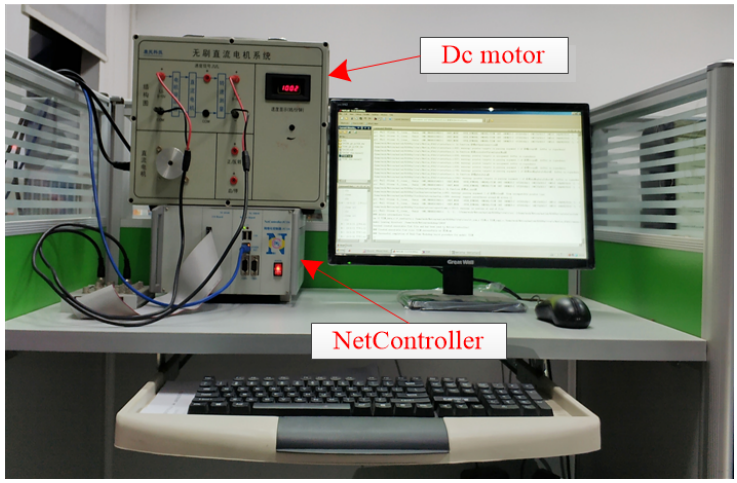

FIGURE 9 DC motor system with NetController plant

The system parameters of the DC motor system mentioned in the numerical simulation part are the same as experiment plant parameters, which are calculated through system identification. The experiment time is set as 60s. The speed tracking results are shown in FIGURE 10 to FIGURE 15.

FIGURE 10 describes the output trajectories of the experimental plant at the speed of 1500rad/min. The differences between these methods are tiny. The proposed control method acts better than the compared method. It has smaller jitters when the system is stable , which is similar the results of the simulation, the convergence speed of HDSMC will faster than DSMC with 16 sample points and the tracking error 3.51 is smaller than the 30.47 of DSMC. Also, when the FDI attack launches, the proposed method reflects quicker.

The control input of the plant at a fixed speed of 1500rad/min is shown in FIGURE 11. When system is attacked and trends to become unstable, both control methods will consume resources to stabilize the system. It is worth noting that the proposed HDSMC consumes less resources and can recover to a stable state faster. FIGURE 12 shows the sliding motion of these two methods. Similarly, the compared method reaches the sliding surface slower and has a

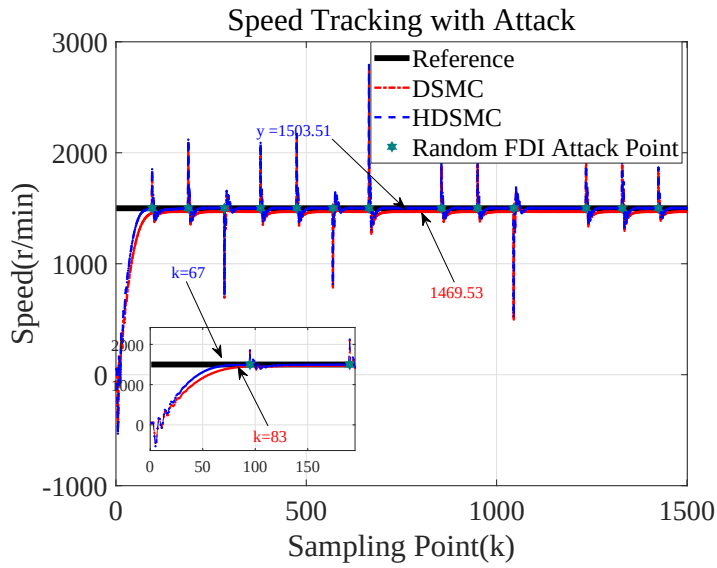

FIGURE 10 Speed tracking of the plant at a fixed speed

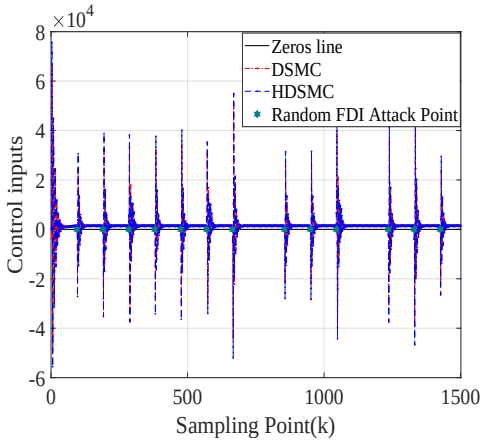

FIGURE 11 Control input of the plant at a fixed speed

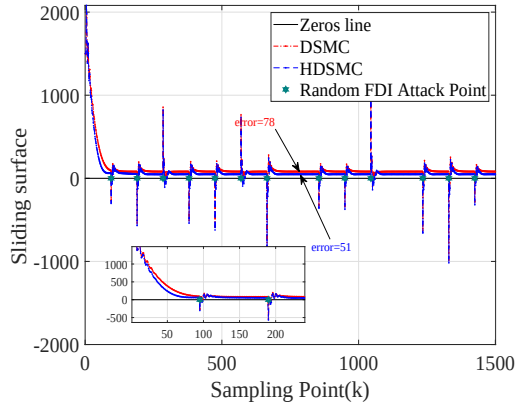

FIGURE 12 Sliding surface of the plant at a fixed speed

larger static error. When an attack occurs, the steady state of the system is destroyed. The proposed HDSMC control method can make the sliding mode motion closer to the sliding mode surface faster and has a smaller approach error 51 than 78 of DSMC.

The tracking control of the plant at changed speed is furtherly carried out to compare the performance of the two different methods, which are shown in FIGURE 13 to FIGURE 15.

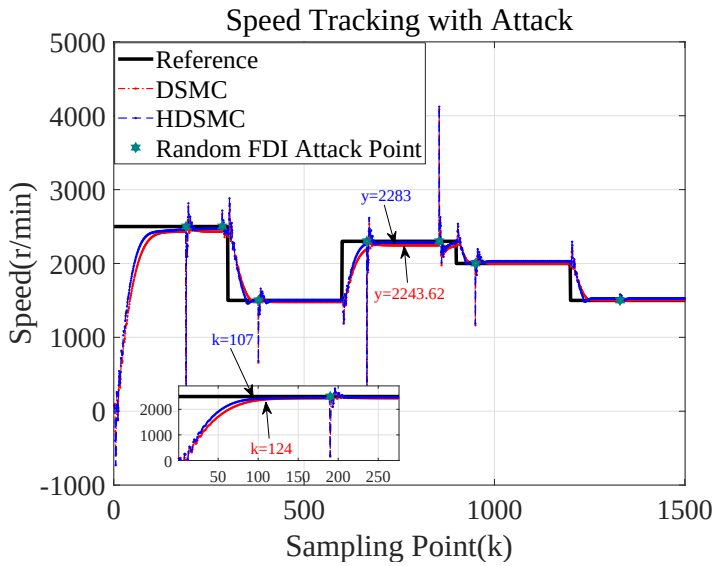

FIGURE 13 Speed tracking of the plant at changed speed

In FIGURE 13, when the system starts to work, the compared one has an obvious tracking error at the reference speed of 2500 rad/min. Also, it tracks slower than the proposed method. When the system deviates from the steady state after an attack, the compared method takes a long time to recover to a stable tracking state.

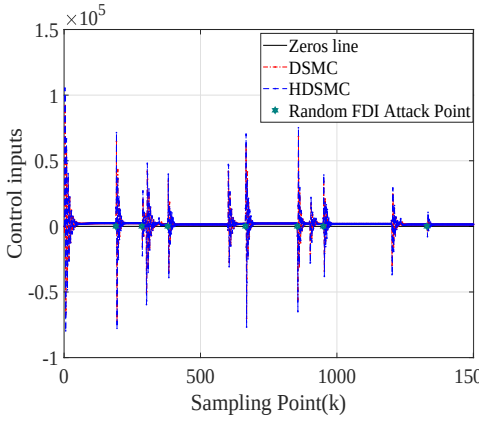

FIGURE 14 Control input of the plant at changed speed

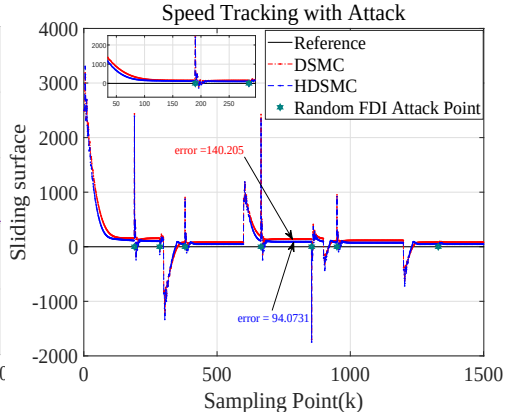

FIGURE 15 Sliding surface of the plant at changed speed

FIGURE 14 shows the control input trajectories with the reference speed varying from 1500 rad/min to 2500

rad/min. Results illustrate that the proposed control strategy jitters smaller when speed changes and an attack happens. FIGURE 15 presents the sliding motion of these two ways. The proposed one response quicker 17 sample points and tracks better with 17 tracking error and less than the tracking error 56 of DSMC . Similar to the simulation results, the proposed method has better characteristics. When an attack occurs, the proposed method consumes less control resources and restores the sliding mode movement to a balanced state faster. Similarly, the sliding mode movement has a smaller jitter bandwidth at this time, so the static jitter page of the entire system is smaller. All the conclusions prove the effectiveness of the proposed method.

6 | CONCLUSION

In this paper, a networked control system with external disturbance and FDI attacks is considered. The instability and jitters are introduced. To solve these problems, firstly the system is researched and modeled. Then, an extended functional observer is presented to observe the states and suppress the effect of FDI attacks and external disturbances. The stability of the observer is proofed. Furthermore, a hybrid control method based on discrete-time sliding mode control and the super-twisting algorithm is presented. The reachability of sliding surface and convergence in finite steps are testified. In the end, the proposed control method is carried out on numerical simulations and practical experiments. Both Results show the reliability and effectiveness of the proposed method in this paper. However, the content studied in this paper still has certain limitations. The control object studied in this paper is a linear time-varying system, and there may be many nonlinear and time-varying systems in actual engineering. In addition, this article focuses on how to quickly restore stability after being attacked. In the future, research can also focus on intrusion detection.

REFERENCES

[1] Bahraini M, Zanon M, Colombo A, Falcone P. Optimal Control Design for Perturbed Constrained Networked Control Systems. IEEE Control Systems Letters 2020;5(2):553–558.

[2] Chang XH, Wang YM. Peak-to-peak filtering for networked nonlinear DC motor systems with quantization. IEEE Transactions on Industrial Informatics 2018;14(12):5378–5388.

[3] Wang L, Yang R, Zhang H. Improved event-triggered sliding mode control of switched systems with disturbances. Asian Journal of Control 2021;23(5):2214–2226.

[4] Qi N, Yuan Q, Liu Y, Huo M, Cao S. Consensus vibration control for large flexible structures of spacecraft with modified positive position feedback control. IEEE Transactions on Control Systems Technology 2018;27(4):1712–1719.

[5] Peng C, Sun H. Switching-like event-triggered control for networked control systems under malicious denial of service attacks. IEEE Transactions on Automatic Control 2020;65(9):3943–3949.

[6] Hu S, Yue D, Han QL, Xie X, Chen X, Dou C. Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. IEEE transactions on cybernetics 2019;50(5):1952–1964.

[7] Niu H, Bhowmick C, Jagannathan S. Attack detection and approximation in nonlinear networked control systems using neural networks. IEEE transactions on neural networks and learning systems 2019;31(1):235–245.

[8] Mao Y, Jafarnejadsani H, Zhao P, Akyol E, Hovakimyan N. Novel stealthy attack and defense strategies for networked control systems. IEEE Transactions on Automatic Control 2020;65(9):3847–3862.

[9] Gao L, Chen B, Yu L. Fusion-based FDI attack detection in cyber-physical systems. IEEE Transactions on Circuits and Systems II: Express Briefs 2019;67(8):1487–1491.

[10] Pang ZH, Liu GP, Zhou D, Hou F, Sun D. Two-channel false data injection attacks against output tracking control of networked systems. IEEE Transactions on Industrial Electronics 2016;63(5):3242–3251.

[11] Abbaspour A, Sargolzaei A, Forouzannezhad P, Yen KK, Sarwat AI. Resilient Control Design for Load Frequency Control System Under False Data Injection Attacks. IEEE Transactions on Industrial Electronics 2020;67(9):7951–7962.

[12] Pang ZH, Liu GP, Zhou D, Hou F, Sun D. Two-Channel False Data Injection Attacks Against Output Tracking Control of Networked Systems. IEEE Transactions on Industrial Electronics 2016;63(5):3242–3251.

[13] Zhao F, Yao H, Chen X, Cao J, Qiu J. Robust H∞ Sliding Mode Control for a Class of Singular Stochastic Nonlinear Systems. Asian Journal of Control 2019;21(1):397–404.

[14] Li M, Chen Y. Wide-area robust sliding mode controller for power systems with false data injection attacks. IEEE Transactions on Smart Grid 2019;11(2):922–930.

[15] Li Z, Zhou S, Xiao Y, Wang L. Sensorless vector control of permanent magnet synchronous linear motor based on self-adaptive super-twisting sliding mode controller. IEEE Access 2019;7:44998–45011.

[16] Li J, Niu Y. Output-feedback-based sliding mode control for networked control systems subject to packet loss and quantization. Asian Journal of Control 2021;23(1):289–297.

[17] Gao P, Zhang G, Ouyang H, Mei L. An adaptive super twisting nonlinear fractional order PID sliding mode control of permanent magnet synchronous motor speed regulation system based on extended state observer. IEEE Access 2020;8:53498–53510.

[18] Lin X, Wang Y, Liu Y. Neural-network-based robust terminal sliding-mode control of quadrotor. Asian Journal of Control 2022;24(1):427–438.

[19] Yao X, Park JH, Dong H, Guo L, Lin X. Robust adaptive nonsingular terminal sliding mode control for automatic train operation. IEEE Transactions on Systems, Man, and Cybernetics: Systems 2018;49(12):2406–2415.

[20] Sun G, Ma Z, Yu J. Discrete-time fractional order terminal sliding mode tracking control for linear motor. IEEE Transactions on Industrial Electronics 2017;65(4):3386–3394.

[21] Xu Q. Piezoelectric nanopositioning control using second-order discrete-time terminal sliding-mode strategy. IEEE Transactions on industrial electronics 2015;62(12):7738–7748.

[22] Bartoszewicz A, Adamiak K. Discrete-time sliding-mode control with a desired switching variable generator. IEEE Transactions on Automatic Control 2019;65(4):1807–1814.

[23] Liu N, Fei J. Adaptive fractional sliding mode control of active power filter based on dual RBF neural networks. IEEE Access 2017;5:27590–27598.

[24] Ge X, Han QL, Zhang XM, Ding D, Yang F. Resilient and secure remote monitoring for a class of cyber-physical systems against attacks. Information Sciences 2020;512:1592–1605.

[25] Orlov Y, Chakrabarty S, Zhao D, Spurgeon SK. Sliding Mode Observer Design for a Parabolic PDE in the Presence of Unknown Inputs. Asian Journal of Control 2019;21(1):224–235.

[26] Li Y, Shi D, Chen T. False Data Injection Attacks on Networked Control Systems: A Stackelberg Game Analysis. IEEE Transactions on Automatic Control 2018;63(10):3503–3509.

[27] Hu L, Wang Z, Han QL, Liu X. State estimation under false data injection attacks: Security analysis and system protection. Automatica 2018;87:176–183.

[28] Liu L, Bi M, Xiao S, Fang J, Huang T, Hu W. OLS-based RBF neural network for nonlinear and linear impairments compensation in the CO-OFDM system. IEEE Photonics Journal 2018;10(2):1–8.

[29] Li M, Chen Y. Robust adaptive sliding mode control for switched networked control systems with disturbance and faults. IEEE Transactions on Industrial Informatics 2018;15(1):193–204.