Int. J. Appl. Math. Comput. Sci., 2026, Vol. 36, No. 1, 81–90
DOI: 10.61822/amcs-2026-0007

EVENT–TRIGGERED NEURAL NETWORK VOLTAGE CONTROL FOR DISTRIBUTION NETWORKS UNDER ACTUATOR ATTACKS BASED ON OBSERVERS

FANG ZHANG [a]

[a] School of Automation
Beijing Information Science and Technology University
No. 55 Taihang Road, Changping District, Beijing, China
e-mail: zhfang101@163.com

This paper proposes an event-triggered neural network control approach to address the voltage control issue in distribution networks under false data injection (FDI) attacks. Firstly, a mathematical model of voltage deviation in distribution networks considering the impact of FDI attacks is established to accurately represent the dynamic behavior of the attacked system. To optimize the utilization of communication resources within the network, an adaptive event-triggered mechanism is designed, which can dynamically adjust the triggering conditions based on the system state, effectively reducing unnecessary communication instances. On this basis, an event-triggered voltage control (VC) system model is established. To effectively mitigate voltage over limit caused by FDI attacks, an adaptive neural network controller is designed, which can compensate for the attack signals and keep the voltage within the allowable range. By combining Lyapunov–Krasovskii stability theory with linear matrix inequality (LMI) techniques, the stability of the system is analyzed, and sufficient conditions for ensuring it are derived. Finally, simulation results demonstrate that this method can not only effectively resist FDI attacks, but also significantly reduce the communication burden while ensuring system stability.

Keywords: distribution network, voltage control, voltage over limit, event-triggered, adaptive neural network.

1. Introduction

In power systems, the distribution network voltage control (DN-VC) system is a widely employed component across power transmission and distribution networks, industrial production setups, and transportation systems. Its prevalence stems from its capability to monitor and adjust voltage levels in real-time with high precision, ensuring the stability and quality of power supply (Zhou *et al.*, 2022; Jamroen, 2022; Murray *et al.*, 2021). The seamless functioning of these systems is heavily reliant on the robustness and security of the DN-VC system, which is paramount for maintaining power quality standards. However, amidst the rapid advancements in smart grid technology, the DN-VC system confronts growing challenges, notably in the realms of network security and resource limitations. These challenges have emerged as pivotal barriers hindering the enhancement of system performance, as well as its safe and stable operation. Consequently, addressing these issues has become imperative for the continued effectiveness and reliability of the DN-VC system in modern power systems (Mohan *et al.*, 2020; Sarkar *et al.*, 2022; Li and Yan, 2020).

Firstly, the deep integration of power networks with IT has made the DN-VC system vulnerable to cyber-attacks (Pang *et al.*, 2023; Zhang *et al.*, 2021; Liang *et al.*, 2016; Yang *et al.*, 2023). Attackers exploit vulnerabilities in the technical network, security measures, and communication protocols to launch targeted attacks, particularly false data injection attacks (FDIAs) on actuators (Duo *et al.*, 2022). These FDIAs involve injecting false information into the actuator's communication channel, affecting voltage and other critical parameters. Industrial control system protocols, due to inherent vulnerabilities and lack of security, are susceptible to cyber-attacks. For instance, the Modbus protocol lacks authentication, encryption, and session integrity (Guo *et al.*, 2023), allowing FDI attackers to tamper with data. Similarly, the widely used DNP3 protocol in power systems can be exploited by attackers

to obtain system configuration information and launch targeted attacks (Gong *et al*., 2023). Successful FDI attacks can lead to false actuator signals and voltage over-limit issues (Husnoo *et al*., 2023; Xing and Liu, 2022). While research has focused on attack detection and state estimation (Aoufi *et al*., 2020; Zhu *et al*., 2022), there is a gap in control-theoretic approaches to mitigate these attacks. Although Hao *et al*. (2024) proposed a distributed intrusion detection method, further exploration into control strategies to enhance the DN-VC system's resilience against cyber-attacks is crucial.

As power systems integrate more intelligent devices, data exchange surges, challenging grid transmission capabilities. Limited network bandwidth and communication resources may lead to data delays or losses, affecting voltage control precision and responsiveness (Zhao, 2024; Sun *et al*., 2019; Choi *et al*., 2021). To address these issues, event-triggered communication (ETC) has gained attention. Unlike conventional time-triggered methods, ETC selectively transmits data based on control requirements, minimizing communication frequency and enhancing system efficiency. This preserves critical data integrity, maintaining system stability, performance, and responsiveness, solving issues related to limited communication in modern power grids (Shi *et al.*, 2019; Liu *et al.*, 2018; 2024).

Inspired by prior studies, this paper explores collaborative design of communication and security in a distribution network's voltage control, proposing an adaptive event-triggered mechanism (A-ETM) to conserve resources and account for delays. It also uses neural networks to estimate attack signals and develop a controller that enhances system resilience. Key contributions are summarized as follows.

- An A-ETM with an upper bound is designed to effectively save communication resources and ensure system performance. Compared with traditional ETMs (Li *et al*., 2022; Aicha and Ahmed, 2024; Guo *et al*., 2024), the A-ETM ensures that, even in extreme situations, the system can maintain a certain monitoring and adjustment capability by setting an upper bound on the triggering threshold, thereby improving the robustness and reliability of the system. Moreover, in this paper, the use of a discrete time period sampling ETM can naturally exclude Zeno behaviour.
- An adaptive neural network control strategy is designed to compensate for voltage deviations under actuator FDI attacks, ensuring the stability and performance of the VC system in the distribution network. Unlike most existing attacks on FDI with probability or energy constraints (Moudoud *et al*., 2022; Lei *et al*., 2022), our proposed neural network-based approach eliminates such special assumptions. Adaptive neural network control can more flexibly handle complex actuator attack scenarios, effectively compensate for voltage deviations caused by attack signals, and enhance the system's ability to resist attacks. Furthermore, the adaptive control scheme is just an extra augmented security element not altering the original controller, and it is easy to work in a "plug-and-play" way.
- The integrated event-triggered adaptive control strategy ensures security and stable control of the voltage control system while effectively conserving communication resources.

The article is organized as follows. Section 2 establishes a voltage deviation model for distribution networks under actuator attacks and introduces an adaptive event-triggered transmission scheme to characterize voltage amplitude deviations. Additionally, an adaptive neural network controller is devised to compensate for the attack signals. Section 3 presents the key outcomes of our analysis, including stability assessments, the design of control laws, and the synthesis of the proposed adaptive event-triggered neural network control scheme. In Section 4, we demonstrate the effectiveness of our security approach through simulation examples. Finally, Section 5 concludes the paper, summarizing the main findings and contributions.

2. Problem formulations

As shown in Fig. 1, when the actuator (voltage regulator) of the VC system in the distribution network is attacked by FDI, it will generate erroneous adjustment signals, resulting in voltage over-limit problems. Moreover, the sensor and actuator signals of the system are transmitted through the network, which may cause serious resource limitations. Therefore, an event-triggered adaptive neural-network voltage control scheme is designed in this paper.

2.1. Voltage control system under an actuator attack.

Specifically, the FDI attack signal will cause voltage fluctuations at each node of the distribution network. Therefore, we assume that $n = 1, 2, \ldots, N$ represents the node sequence number of the distribution network, and $\Delta V_n(k)$ is the voltage deviation of the n-th node at time k. Letting

$$\begin{aligned}\chi(k) &= \Delta V(k) \\ &= \left[\ \Delta V_1(k),\quad \Delta V_2(k),\quad \ldots,\quad \Delta V_N(k)\ \right]^T,\end{aligned}$$

the dynamic relationship between the voltage deviation of the distribution network and the actuator attack is as follows:

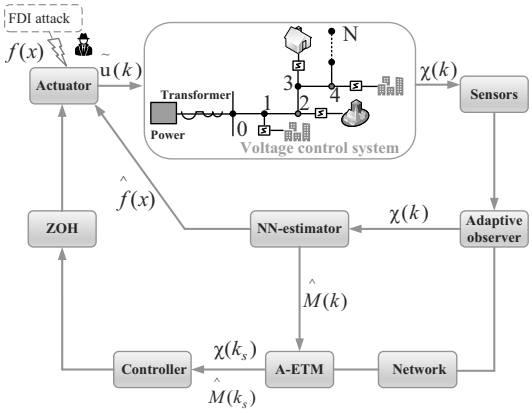

Fig. 1. Security control framework of a voltage control system.

$$\begin{cases} \chi(k+1) = \mathcal{A}\chi(k) + \mathcal{B}\tilde{u}(k), \\ \tilde{u}(k) = u(k) + f(\chi(k)), \end{cases} \tag{1}$$

where $\chi(k)$ is the state vector containing the voltage deviation of all nodes, $\mathcal{A}$ is the system matrix, $\mathcal{B}$ is the input matrix that describes the effect of the actuator on the voltage, $\tilde{u}(k)$ is the actual input signal under FDI attacks, $u(k)$ is the control input vector of the actuator, and $f(\chi(k))$ is an arbitrary FDI by attackers. It is assumed that $(\mathcal{A}, \mathcal{B})$ is controllable. For convenience, we abbreviated $f(\chi(k))$ to $f(\chi)$.

Remark 1. It is noteworthy that the neural-network technology utilized in this paper possesses robust nonlinear mapping capabilities, enabling it to approximate any complex nonlinear system. As a result, contrary to probabilistic assumptions or energy constraints employed in the majority of research (Zhang *et al.*, 2023; He *et al.*, 2022), we did not make any binding assumptions regarding the attack signal. Therefore, the security control strategy proposed in this paper is practical.

In addition, we propose a state-dependent attack-signal based method for characterizing FDI attacks, which gets rid of the probabilistic and periodic dependence of traditional NCS security modelling methods on the attack signal, and therefore, the attack signal $f(x)$ is a system state-dependent function. Therefore, the proposed method is more practical.

2.2. Design of an adaptive neural network estimator. In order to offset the impact of the attack signal on the system, we apply the NN technique to approach the attack signal $f(\chi)$ as

$$f(\chi) = M^T S(\chi) + \varepsilon(\chi), \quad \chi \in \Lambda \subset \mathbb{R}^n, \tag{2}$$

where Λ expresses a compact set, $M \in \mathbb{R}^{p\times m}$ is an ideal constant weight matrix, p is the number of NN nodes, and $\varepsilon(\chi)$ denotes the NN approximation error in which $\|\varepsilon(\cdot)\| \le \bar{\varepsilon}$. The basis function

$$S(\chi) = \begin{bmatrix} s_1(\chi) & s_2(\chi) & \cdots & s_p(\chi) \end{bmatrix}^T \tag{3}$$

satisfies $\|S(\cdot)\| \le S_{\max}$, in which $S_{\max}$ is a positive constant, while $s_i(\chi)$ can be represented as

$$s_i(\chi) = \exp(-\frac{\|\chi - g_i\|^2}{z_i}), \tag{4}$$

where g_i and z_i are the center and width of function $s_i(\chi)$, $g_i = \begin{bmatrix} g_{i1} & g_{i2} & \cdots & g_{i3} \end{bmatrix}^T$.

Moreover, the estimation $\hat{f}(\chi)$ of the deception attack signal $f(\chi)$ is constructed as

$$\hat{f}(\chi) = \hat{M}^T(k) S(\chi(k)), \tag{5}$$

where $\hat{M}(k)$ is the estimation of M. Then, the adaptive law $\hat{M}$ is designed as follows:

$$\hat{M}(k+1) = -\lambda\hat{M}(k) + \hat{M}(k) - \rho\eta(k)\chi^T(k)H^T, \tag{6}$$

where $\lambda > 0$ and $\rho > 0$ are two constants, $H \in \mathbb{R}^{n\times m}$ is an adjustment parameter and

$$\eta(k) = S(\chi(k))/(1 + \|S(\chi(k))\|^2\|H\chi(k)\|^2). \tag{7}$$

Define the estimation error $\tilde{M}(k) = \hat{M}(k) - M$; then we have

$$\tilde{M}(k+1) = -\lambda\hat{M}(k) + \tilde{M}(k) - \rho\eta(k)\chi^T(k)H^T. \tag{8}$$

2.3. Design of the A-ETM and a neural network feedback controller. In this subsection, in order to save communication resources, we design an A-ETM with a system state and parameter estimation signal, as well as a neural network feedback controller. Finally, a closed-loop control system based on event triggering is constructed. The A-ETM structure is as follows (Sun *et al.*, 2023; Chen and Zou, 2023):

$$\begin{aligned} k_{s+1} = \inf_k \{k_s < k | e^T(k)\Phi e(k) \ge \frac{\theta_1}{1 + \|\chi(k_s)\|} \\ \chi^T(k_s)\Phi\chi(k_s) \vee \|E(k)\|_F^2 \ge \theta_2\|\hat{M}(k)\|_F^2\}, \end{aligned} \tag{9}$$

where $e(k)$ denotes the sampled-data error between the current measured output $\chi(k)$ and the last released one $\chi(k_s)(s = 0, 1, 2, \ldots)$, k_s is the last event-triggered time, and k_{s+1} is the next triggering time. $E(k) = \hat{M}(k) - \hat{M}(k_s)$ indicates the data error between the current estimated signal parameters and the last estimated signal parameters. Φ is the corresponding weight matrix to be designed later, while $1 > \theta_1 > 0$ and $1 > \theta_2 > 0$ are the event-triggered parameters.

Remark 2. The design of the event-triggered mechanism is to introduce the system state $\chi(k_s)$ into the threshold of the event-triggered condition, so that the event triggering threshold can be dynamically adjusted according to the state of the VC system. From the mathematical expression of the A-ETM, the event-triggered mechanism has the following characteristics:

- First, $\theta_1 > 0$ avoids the denominator of the event trigger threshold function being zero, thereby ensuring that the designed event-triggered function has mathematical significance.
- If θ_1 and θ_2 are properly designed, all event-triggered transmissions can meet the stability conditions of the control system and can be adjusted to send data at an appropriate frequency.
- When the system states are unstable, $\|\chi(k_s)\|$ will increase, resulting in a smaller event-triggered threshold and faster transmission frequency, enhancing the ability to control and regulate the system. Conversely, it can save network resources.
- When the system status are stable, $\|\chi(k_s)\|$ decreases, resulting in a larger event trigger threshold and slower transmission frequency, thus saving network resources.

Remark 3. Based on the above analysis, it is clear that the A-ETM designed in this paper has the following advantages:

- *Dynamic threshold adjustment:* Unlike traditional event-triggered mechanisms that employ fixed triggering thresholds (Guo *et al*., 2023; Gong *et al*., 2023), our A-ETM dynamically adjusts its triggering conditions based on the system state ($\chi(k_s)$). This feature allows the mechanism to adapt to the changing conditions of the DN-VC system, thereby improving the robustness and responsiveness of the control system.
- *Bounded threshold:* To ensure the system's performance even in extreme situations, we designed the A-ETM with an upper bound on the triggering threshold. This means that the system can maintain a certain level of monitoring and adjustment capability, even when the state deviations become large, enhancing the reliability of the overall control system.
- *Handling complex attack:* The adaptive nature of the A-ETM, combined with the flexibility of the neural network controller, enables our approach to effectively handle complex actuator attack scenarios. This is achieved by dynamically adjusting the communication frequency and the control input based on the evolving system state and estimated attack signals.

However, the A-ETM proposed in this paper is committed to saving communication resources while ensuring the stability of the control system and cannot guarantee the reduction of communication loss, link degradation and other problems. Therefore, it is necessary to study more flexible event-triggered strategies in the future to further improve the applicability of the event-triggered mechanism.

According to Fig. 1, by combining the neural network estimation (5), we design the adaptive neural network feedback controller as

$$u(k) = \mathcal{K}\chi(k_s) - \hat{f}(\chi), \tag{10}$$

where $\mathcal{K}$ is the is the feedback controller gain to be determined and $\hat{f}(\chi)$ is the estimation of the attack signal $f(\chi)$.

By means of the above analysis, considering (1), (2), (5), (9), and (10), the system is represented as

$$\begin{cases} \chi(k+1) = \mathcal{A}\chi(k) + \mathcal{B}\mathcal{K}\chi(k) + \mathcal{B}\mathcal{K}e(k) + \mathcal{B}\varepsilon(\chi(k)) \\ \qquad\qquad -\mathcal{B}\tilde{M}(k)S(\chi(k)) \\ \text{subject to A-ETM (9)} \end{cases} \tag{11}$$

for $k \in [k_s, k_{s+1})$.

3. Results

In this section, the sufficient conditions for the system (11) to be semi-globally uniformly ultimately bounded (SGUUB) are presented using the new Lyapunov functional. According to these conditions, a co-design strategy of the control gain and event-triggering parameter is proposed.

3.1. Stability analysis under the A-ETM with adaptive NN control.

Theorem 1. *For given positive parameters* μ, δ_1, δ_2, ρ, θ_2, κ_1, κ_2 *and* $0 < \beta < 1$ *satisfying*

$$\digamma_1 = \mu(\frac{1}{4\kappa_2} - \lambda + 1 - \beta) + \delta_1 S_{\max}^2 < 0, \tag{12}$$

$$\digamma_2 = \mu(\lambda^2 - \lambda + \kappa_1) + \theta_2 < 0, \tag{13}$$

$$\digamma_3 = -1 + \delta_2 S_{\max}^2 < 0, \tag{14}$$

$$\digamma = \mu\lambda\|M\|_F^2 + \mu\rho^2(\frac{1}{4} + \frac{\lambda^2}{4\kappa_1} + \kappa_2) + \bar{\varepsilon}^2, \tag{15}$$

if there exist a matrix $\mathcal{K}$ *and a positive parameter* θ_1, *and some symmetric positive definite matrices* P, Φ, R_1, R_2 *with appropriate dimensions satisfying*

$$\Omega = \begin{bmatrix} \Omega_{11} & \Omega_{12} \\ * & -I \end{bmatrix} < 0, \tag{16}$$

where

$$\begin{aligned}\Omega_{11} &= v_1^T(\theta_1\Phi-\beta P)v_1+v_2^TPv_2-v_3^T\Phi v_3-\delta_1 v_4^Tv_4\\ &\quad+He\{(v_1^TR_1+v_2^TR_2)(-\mathcal{B}v_4)\}\\ &\quad+He\{(v_1^TR_1+v_2^TR_2)\\ &\quad\times((\mathcal{A}+\mathcal{B}\mathcal{K})v_1-v_2+\mathcal{B}\mathcal{K}v_3)\},\end{aligned}$$

$$\Omega_{12} = v_1^TR_1\mathcal{B}+v_2^TR_2\mathcal{B},$$

$$\begin{aligned}v_1&=\left[\begin{array}{ccc} I_n & 0_{r\times(2n+m)}\end{array}\right],\\ v_2&=\left[\begin{array}{ccc} 0_{n\times n} & I_n & 0_{n\times(n+m)}\end{array}\right],\\ v_3&=\left[\begin{array}{ccc} 0_{n\times 2n} & I_n & 0_{n\times m}\end{array}\right],\\ v_4&=\left[\begin{array}{cc} 0_{m\times 3n} & I_m\end{array}\right],\end{aligned}$$

then the system (11) is semiglobally uniformly ultimately bounded.

Proof. We choose a Lyapunov–Krasovskii functional as follows:

$$\mathcal{V}(k)=\mathcal{V}_1(k)+\mu\mathcal{V}_2(k), \tag{17}$$

where $\mathcal{V}_1(k)=\chi^T(k)P\chi(k)$ and $\mathcal{V}_2(k)=Tr\{\tilde{M}^T(k)\tilde{M}(k)\}$, and μ is a positive constant.

Then, calculating the differences of $\mathcal{V}_1(k)$ along (11), one obtains

$$\begin{aligned}&\mathcal{V}_1(k+1)-\beta\mathcal{V}_1(k)\\ &\quad=\chi^T(k+1)P\chi(k+1)-\beta\chi^T(k)P\chi(k)\\ &\quad=\xi^T(k)[-\beta v_1^TPv_1+v_2^TPv_2]\xi(k),\end{aligned} \tag{18}$$

where $\xi(k)=col\{\chi(k),\chi(k+1),e(k),\tilde{M}^T(k)S(\chi(k))\}$.

Calculating the difference of $\mathcal{V}_2(k)$ along (6), we obtain

$$\begin{aligned}&\mathcal{V}_2(k+1)-\mathcal{V}_2(k)\\ &=Tr\{\tilde{M}^T(k+1)\tilde{M}(k+1)\}-Tr\{\tilde{M}^T(k)\tilde{M}(k)\}\\ &=Tr\{\lambda^2\hat{M}^T(k)\hat{M}(k)-2\lambda\hat{M}^T(k)\tilde{M}(k)\\ &\quad+2\lambda\rho\hat{M}(k)\eta(k)H\chi(k)-2\rho\tilde{M}(k)\eta(k_s)H\chi(k)\}\\ &\quad+\rho^2\|\eta(k)\|^2\|H\chi(k)\|^2.\end{aligned} \tag{19}$$

According to (7), this yields

$$\|\eta(k)\|^2\|H\chi(k)\|^2\le\frac{1}{4}.$$

Therefore, by applying Young's inequality, if there exist constants $\kappa_1>0$ and $\kappa_2>0$, we can obtain

$$\begin{aligned}&Tr\{2\lambda\rho\hat{M}(k)\eta(k)H\chi(k)\}\\ &\quad\le\kappa_1Tr\{\hat{M}^T(k)\hat{M}(k)\}+\frac{\lambda^2\rho^2}{4\kappa_1}\\ &\qquad-Tr\{2\rho\tilde{M}(k)\eta(k)H\chi(k)\}\\ &\quad\le\frac{Tr\{\tilde{M}^T(k)\tilde{M}(k)\}}{4\kappa_2}+\kappa_2\rho^2.\end{aligned} \tag{20}$$

In addition, according to $\tilde{M}(k)=\hat{M}(k)-M$, one obtains

$$\begin{aligned}&Tr\{-2\lambda\hat{M}^T(k)\tilde{M}(k)\}\\ &=Tr\{\lambda M^TM-\lambda\tilde{M}^T(k)\tilde{M}(k)-\lambda\hat{M}^T(k)\hat{M}(k)\}\end{aligned} \tag{21}$$

Combining (19)–(21), we have

$$\begin{aligned}&\mathcal{V}_2(k+1)-\beta\mathcal{V}_2(k)\\ &\quad\le(\frac{1}{4\kappa_2}-\lambda+1-\beta)\|\tilde{M}(k)\|_F^2\\ &\qquad+\rho^2(\frac{1}{4}+\frac{\lambda^2}{4\kappa_1}+\kappa_2)\\ &\qquad+\lambda\|M\|_F^2+(\lambda^2-\lambda+\kappa_1)\|\hat{M}(k)\|_F^2\end{aligned} \tag{22}$$

If there exist free-weighting matrices R_1 and R_2, we have

$$\begin{aligned}&2[\chi^T(k)R_1+\chi^T(k+1)R_2][(\mathcal{A}+\mathcal{B}\mathcal{K})\chi(k)\\ &\qquad+\mathcal{B}\mathcal{K}e(k)+\mathcal{B}\varepsilon(\chi(k))-\mathcal{B}\tilde{M}(k)\\ &\qquad S(\chi(k))-\chi(k+1)]=0,\end{aligned} \tag{23}$$

where

$$\begin{aligned}&2[\chi^T(k)R_1+\chi^T(k+1)R_2]\mathcal{B}\varepsilon(\chi(k))\\ &\quad\le\xi^T(k)[v_1^TR_1\mathcal{B}+v_2^TR_2\mathcal{B}]\\ &\qquad[v_1^TR_1\mathcal{B}+v_2^TR_2\mathcal{B}]^T\xi(k)+\bar{\varepsilon}^2\end{aligned} \tag{24}$$

With the parameters $\delta_1>0$ and $\delta_2>0$, one can derive that the inequality (25) is greater than zero:

$$\begin{aligned}&\delta_1S_{\max}^2\|\tilde{M}(k)\|_F^2-\delta_1S^T(\chi(k))\tilde{M}(k)\tilde{M}^T(k)S(\chi(k)),\\ &\delta_2S_{\max}^2\|E(k)\|_F^2-\delta_2S^T(\chi(k))E(k)E^T(k)S(\chi(k)).\end{aligned} \tag{25}$$

From the A-ETM (9), we can have that

$$\left\{\begin{array}{l}0\ge-e^T(k)\Phi e(k)+\frac{\theta_1}{1+\|\chi(k_s)\|}\chi^T(k_s)\Phi\chi(k_s),\\ 0\ge-\|E(k)\|_F^2+\theta_2\|\hat{M}(k)\|_F^2.\end{array}\right. \tag{26}$$

Based on the above analysis and using Schur's complement lemma, we get

$$\begin{aligned}&\mathcal{V}(k+1)-\beta\mathcal{V}(k)\le\xi^T(k)\Omega\xi(k)+\digamma\\ &+\digamma_1\|\tilde{M}(k)\|_F^2+\digamma_2\|\hat{M}(k)\|_F^2+\digamma_3\|E(k)\|_F^2.\end{aligned} \tag{27}$$

Because of $\Omega<0$, $\digamma_1<0$, $\digamma_2<0$ and $\digamma_3<0$, we have

$$\mathcal{V}(k+1)\le\beta\mathcal{V}(k)+\digamma, \tag{28}$$

where $\xi(k)=col\{\chi(k),\chi(k+1),e(k),\tilde{M}^T(k)S(\chi(k))\}$.

It can be concluded that, if the LMI (16) holds, then the nominal event-triggered control system (11) is SGUUB. The proof is completed. ■

It is worth noting that Theorem 1 provides semi-globally uniformly bounded conditions for the closed-loop systems (11), considering only the event-triggered parameter θ while maintaining stability. Next, we will apply the matrix operation on the basis of Theorem 1 to obtain the gain $\mathcal{K}$ of the state feedback controller.

Theorem 2. *For given positive parameters μ, δ_1, δ_2, ρ, θ_2, κ_1, κ_2 and $0 < \beta < 1$ satisfying (12)–(14), if there exist a matrix $\mathcal{K}$ and a positive parameter θ_1, and some symmetric positive definite matrices $\bar{P}$, $\bar{\Phi}$, and $\mathcal{X}$ with appropriate dimensions satisfying*

$$\begin{bmatrix} \bar{\Omega}_{11} & \bar{\Omega}_{12} \\ * & -I \end{bmatrix} < 0, \tag{29}$$

where

$$\begin{aligned}\bar{\Omega}_{11} &= v_1^T(\theta_1\bar{\Phi} - \beta\bar{P})v_1 + v_2^T\bar{P}v_2 - v_3^T\bar{\Phi}v_3 - \delta_1 v_4^T v_4 \\ &\quad + He\{(v_1^T + \tau v_2^T)((\mathcal{A}\mathcal{X} + \mathcal{B}\mathcal{Y})v_1 - \mathcal{X}v_2 \\ &\quad + \mathcal{B}\mathcal{Y}v_3)\} + He\{(v_1^T + \tau v_2^T)(-\mathcal{B}v_4)\}, \\ \bar{\Omega}_{12} &= v_1^T\mathcal{B} + \tau v_2^T\mathcal{B},\end{aligned}$$

then the equivalent event-triggered feedback controller's gain can be calculated by

$$\mathcal{K} = \mathcal{Y}\mathcal{X}^{-1}. \tag{30}$$

Proof. Define $\mathcal{X} = (R_1)^{-T}$, $R_2 = \tau R_1$, $\mathcal{Y} = \mathcal{K}\mathcal{X}$, $\bar{P} = \mathcal{X}^T P \mathcal{X}$, $\bar{\Phi} = \mathcal{X}^T \Phi \mathcal{X}$, and $\Pi = diag\begin{bmatrix} \mathcal{X}^T & \mathcal{X}^T & \mathcal{X}^T & I_n \end{bmatrix}$. Pre-and-post multiplying both sides of the matrix inequality (16) with Π and Π^T, we can arrive at the desired results. ■

Theorem 3. *Consider the event-triggered secure control (11) of VC under actuator attacks. The secure adaptive NN controller can be given by*

$$u(k) = \mathcal{Y}\mathcal{X}^{-1}\chi(k_s) - \hat{f}(\chi), \tag{31}$$

where $\hat{f}(\chi) = \hat{M}^T(k)S(\chi(k)) + \varepsilon(\chi(k))$ is an estimation of an abnormal actuator signal with $\hat{M}(k+1) = -\lambda\hat{M}(k) + \hat{M}(k) - \rho\eta(k)\chi^T(k)H^T$.

Proof. Based on Theorems 1 and 2, one can easily obtain the desired result. ■

4. Illustrative examples

To validate the effectiveness and feasibility of the proposed method, this section presents simulations and discussions based on the IEEE-8 node test case. The results demonstrate the practical application and performance of our A-ETM and the adaptive neural network control strategy in real-world scenarios.

Parameter and state matrix setups. As shown in Fig. 2, we adopt an 8-node voltage topological system model.

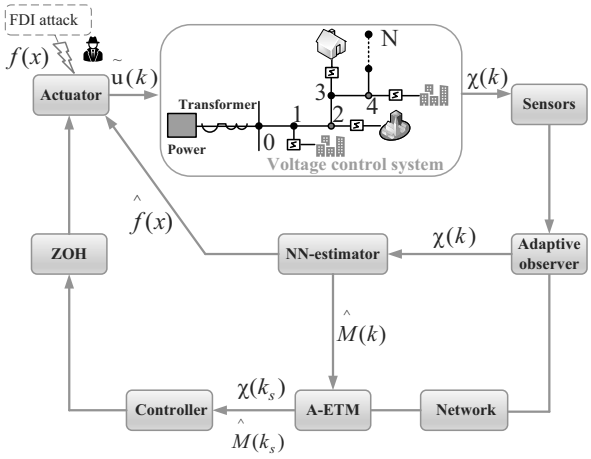

Fig. 2. IEEE-8 node distribution network example power topology.

Assuming that the electrical coupling between the nodes in a simple 8-node distribution network is relatively weak, and the voltage at each node tends to decay towards its reference voltage, we provide the following parameters:

$$\mathcal{A} = \begin{bmatrix} -1.0 & 0.1 & 0.02 & 0.01 \\ 0.05 & -1.0 & 0.25 & 0.02 \\ 0.02 & 0.03 & -1.0 & -0.8 \\ 0.01 & 0.02 & 0.04 & -1.0 \end{bmatrix},$$

$$\mathcal{B} = \begin{bmatrix} 0.2 & 0.15 & 0.2 & 25 \end{bmatrix}^T.$$

Secure control design. Setting the parameters as $\mu = 500$, $\delta_1 = 0.1$, $\delta_2 = 0.01$, $\lambda = 0.8$, $\rho = 0.9$, $\theta_2 = 0.4$, $\kappa_1 = 0.01$, $\kappa_2 = 250$, $\beta = 0.9$ and $S_{\max} = 2$, we can get $\digamma_1 = -349.1$, $\digamma_2 = -74.6$, $\digamma_3 = -0.96$.

Let $\tau = 0.56$, $\theta_1 = 0.1$. According to (13) and using the Matlab LMI toolbox, we can get

$$\mathcal{K} = 10^{-6} \times \begin{bmatrix} 0.0030 & 0.0084 & -0.0054 & -0.1973 \end{bmatrix},$$

$$\Phi = 10^7 \times \begin{bmatrix} 1.9179 & -0.4630 & -0.2692 & 0.0313 \\ -0.4630 & 2.8643 & -1.2059 & -0.0091 \\ -0.2692 & -1.2059 & 0.6245 & -0.0037 \\ 0.0313 & -0.0091 & -0.0037 & 0.0005 \end{bmatrix}.$$

In addition, we set $Q = \begin{bmatrix} 1 & 1 & -1 & -1 \end{bmatrix}$, and we can obtain the adaptive law $\hat{M}(k+1) = 0.2\hat{M}(k) + \hat{M}(k) - 0.6\eta(k)\chi^T(k)H^T$.

The attack signal is selected as $f(\chi) = 1.7\tanh(\chi_1(k)) + 0.07\chi_1(k_s)/(1 + \chi_1^2(k_s))$. Suppose that the NN consists of five nodes. Let the compact set be $\Lambda = [-2, 2]^5$, where the centers are uniformly distributed. The widths are chosen as $z_i = 4$ with $i \in \{1, \ldots, 5\}$. The initial value of $\hat{M}(0) = 0_{5\times 1}$.

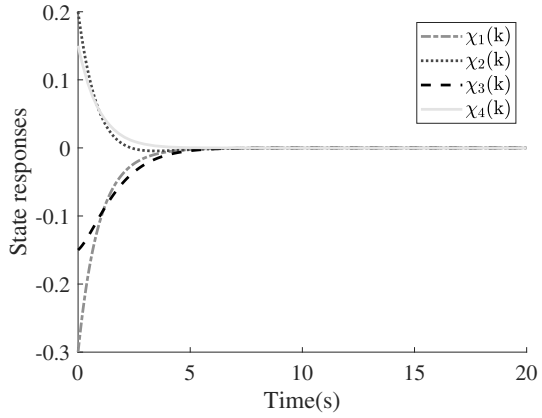

Fig. 3. State responses of DN-VC in Part A.

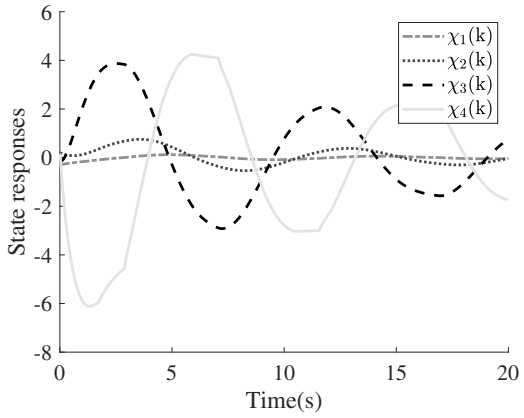

Fig. 5. State responses of DN-VC in Part B.

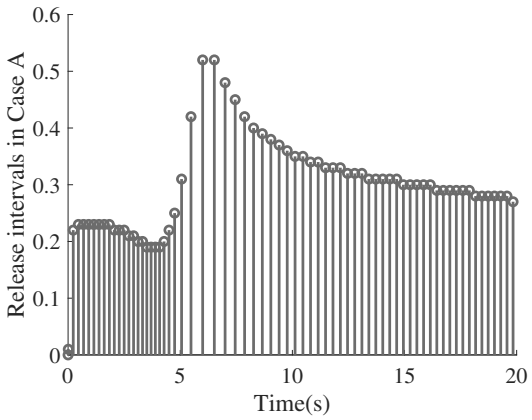

Fig. 4. Release intervals in Part A.

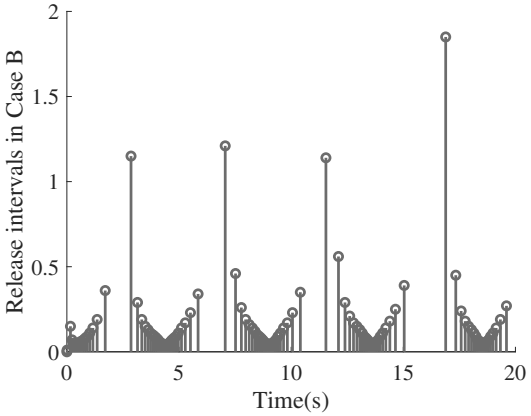

Fig. 6. Release intervals in Part B.

Finally, the sampling period is given by $h = 0.01$ s, and the total simulation time is set as $T = 20$ s.

Based on the above setups, we can get the following simulation results.

Results comparisons and analysis. In this section, the following simulation results are compared to highlight the effectiveness of the proposed adaptive control scheme. Part A shows the system status without an actuator attack and additional auxiliary control scheme. Part B shows the malicious effects of an actuator attack without adaptive security control scheme. Part C uses the designed adaptive neural network feedback controller to correct the actuator attack signal, which verifies the effectiveness of the proposed adaptive control method based on the A-ETM for cooperative communication and control.

Part A: Without actuator attacks under $u(k) = \mathcal{K}\chi(k_s)$. In Part A, we assume that no actuator attacks occurred and no additional auxiliary secure design is performed. Then, under $u(k) = \mathcal{K}\chi(k_s)$, the state responses of DN-VC are shown in Fig. 3. It can be clearly seen there that the voltage deviation gradually approaches zero when there is no actuator attack, indicating that the traditional event-triggered feedback controller can ensure the stability of the DN-VC system when there is no actuator attack. From Fig. 4, it can be observed that the number of transmissions is 68 times, and the effect of the adaptive event triggering strategy can be seen from the transmission interval.

Part B: Actuator attacks under $u(k) = \mathcal{K}\chi(k_s)$. In Part B, considering that the actuator of the DN-VC system is attacked by false data injection $f(\chi) = 1.7tanh(\chi_1(k)) + 0.07\chi_1(k_s)/(1 + \chi_1^2(k_s))$, the traditional event-triggered feed-back controller $u(k) = \mathcal{K}\chi(k_s)$ is adopted. As seen in Fig. 5 and 6, we get the voltage deviation state and data transmission frequency of the system. As shown in Fig. 5, the large fluctuation in the amplitude of voltage deviation indicates that the traditional event-triggered feedback controller cannot guarantee the stability of the DN-VC system under actuator attacks. From Fig. 6, it can be observed that, when the system state is unstable, the frequency of system data transmission increases, verifying that the event-triggered threshold is adaptively adjusted

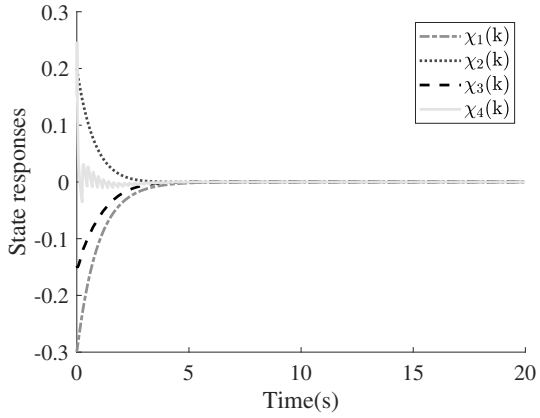

Fig. 7. State responses and the switching controller signal in Part C.

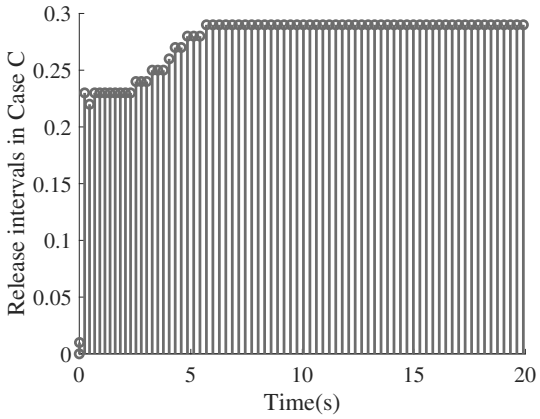

Fig. 8. Release intervals in Part C.

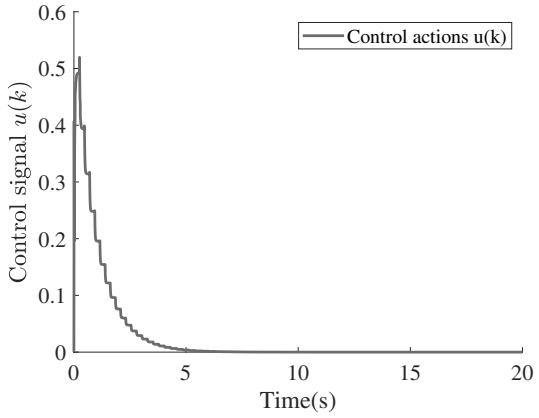

Fig. 9. Response of the control law in Part C.

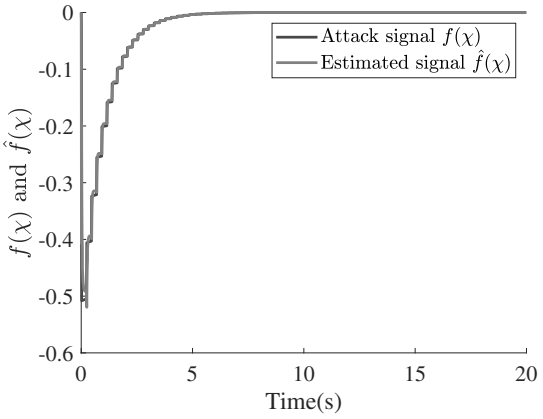

Fig. 10. Estimation of $f(x(k))$ using an NN.

based on the system state. Furthermore, the number of transmissions is 127 times, significantly reducing the data transmission frequency compared to the time-triggered mechanism.

Part C: Actuator attacks under $u(k) = \mathcal{K}\chi(k_s) - \hat{f}(\chi)$. Lastly, when the DN-VC system is subjected to actuator attacks, we utilize the proposed secure adaptive state feedback controller $u(k) = \mathcal{K}\chi(k_s) - \hat{f}(\chi)$ to validate the effectiveness of this approach. As illustrated in Fig. 7, with the designed secure controller in action, the voltage error of the system gradually converges to zero, indicating that the A-ETM adaptive neural network control strategy achieves superior stability. Figure 8 demonstrates the effectiveness of the event-triggering mechanism. It can be seen that the A-ETM can efficiently schedule communication resources. Figure 9 shows the corresponding control signal output from the controller. Figure 10 presents the approximation effect of the neural network technology on the attack signal. It can be seen that the output signal of the estimator can well approximate the attack signal of the malicious actuator. It is evident from the comparison of Parts A, B and C that the integrated secure adaptive control strategy $u(k)$ derived from Theorem 3 effectively mitigates the impact of actuator attacks on the DN-VC system. Furthermore, the above examples demonstrate the significant advantage of the event-triggered strategy in conserving communication resources.

Remark 4. In order to validate the superiority of the adaptive control based on event-triggered strategy proposed in this paper, we selected two attack signals, namely, Signal A and Signal B, for testing: $Signal\, A = 0.7\cos(x_2(k)) - 4.2\tanh(x_1(k))$ and $Signal\, B = 3x_2(k)/(1 + x_2^2(k))$. The obtained results are shown in the figures as follows. Figure 11 depicts the state of the voltage system under the attack of attack signal A with the tracking state of the adaptive control signal to attack A. Figure 12 illustrates the state of the voltage system under the attack of attack Signal B with the tracking state of the adaptive control signal to attack Signal B. It can be seen that our proposed safety control strategy can stabilize the voltage control system in time under the influence of different attack signals.

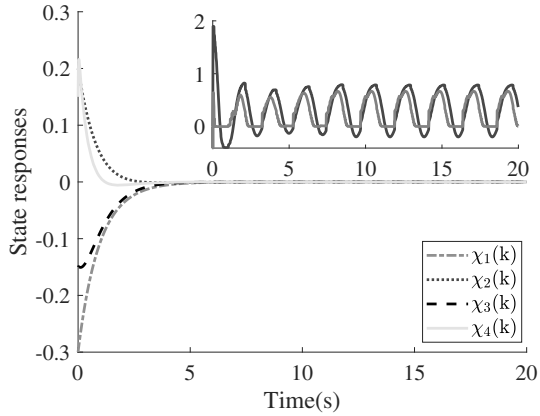

Fig. 11. State responses and a tracking signal to attack A.

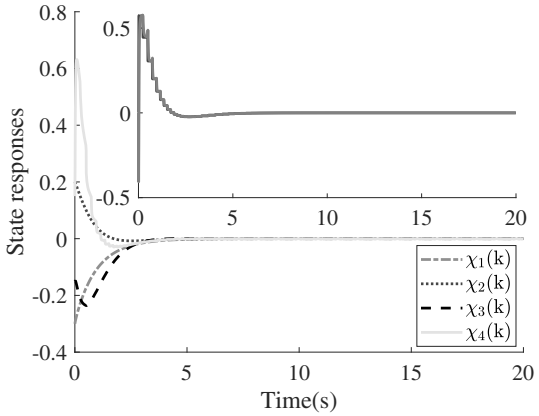

Fig. 12. State responses and a tracking signal to attack B.

5. Conclusions

The security control issue of voltage control systems in distribution networks under actuator attacks was investigated. Firstly, a voltage deviation model under actuator attacks was established. Secondly, to more effectively conserve network communication resources within a limited bandwidth, an adaptive event-triggered transmission scheme with upper bounds was proposed. Then, an adaptive neural network control strategy was designed to mitigate actuator attacks. The neural network technology was utilized to approximate the attack signals, which was subsequently compensated for in the actuator attack signals. By leveraging the Lyapunov–Krasovskii method and solving a set of (LMIs), stability criteria and the stabilization methods for the voltage control system were obtained. Finally, the effectiveness of the proposed security control method was verified through simulation examples.

However, the control strategy in this paper is still centralized, and its computational load and reliability will decline with the increase of the scale. It is necessary to study distributed control strategies in the future to further improve the robustness and economy of the distribution network operation. In addition, the neural network technique proposed in this paper does not consider the size and structure of the neural network for the time being, and in our future work, we will further explore how to optimise the structure and parameters of the neural network according to different application scenarios and system requirements in order to improve its practicality and performance.

References

Aicha, Z. and Ahmed, S.N. (2024). Decentralized sliding mode control using an event-triggered mechanism for discrete interconnected Hammerstein systems, *International Journal of Applied Mathematics and Computer Science* **34**(3): 349–360, DOI: 10.61822/amcs-2024-0025.

Aoufi, S., Derhab, A. and Guerroumi, M. (2020). Survey of false data injection in smart power grid: Attacks, countermeasures and challenges, *Journal of Information Security and Applications* **54**: 102518, DOI: 10.1016/j.jisa.2020.102518.

Chen, C. and Zou, W. (2023). Event-triggered consensus of multiple uncertain Euler–Lagrange systems with limited communication range, *IEEE Transactions on Systems, Man, and Cybernetics: Systems* **53**(9): 5945–5954.

Choi, J., Habibi, S. and Bidram, A. (2021). Distributed finite-time event-triggered frequency and voltage control of AC microgrids, *IEEE Transactions on Power Systems* **37**(3): 1979–1994.

Duo, W., Zhou, M. and Abusorrah, A. (2022). A survey of cyber attacks on cyber physical systems: Recent advances and challenges, *IEEE/CAA Journal of Automatica Sinica* **9**(5): 784–800.

Gong, S., Zheng, M., Hu, J. and Zhang, A. (2023). Event-triggered cooperative control for high-order nonlinear multi-agent systems with finite-time consensus, *International Journal of Applied Mathematics and Computer Science* **33**(3): 439–448, DOI: 10.34768/amcs-2023-0032.

Guo, G., An, X., Sun, J., Ji, Z. and Zhao, Z. (2023). Observer-based event-triggered sliding mode tracking control for uncertain robotic manipulator systems, *Journal of the Brazilian Society of Mechanical Sciences and Engineering* **45**(9): 453.

Guo, G., Tan, H., Feng, Y. and Wang, Y. (2024). Event-triggered fixed-time tracking control for uncertain networked autonomous surface vehicle with disturbances, *Ocean Engineering* **312**(1): 119100.

Hao, M., Lan, J., Wang, L., Lin, Y., Wang, J. and Qin, L. (2024). Optimized dual-layer distributed energy storage configuration for voltage over-limit zoning governance in distribution networks, *Energies* **17**(8): 1847.

He, N., Ma, K. and Li, H. (2022). Resilient predictive control strategy of cyber-physical systems against FDI attack, *IET Control Theory & Applications* **16**(11): 1098–1109.

Husnoo, M., Anwar, A., Hosseinzadeh, N., Islam, S., Mahmood, A. and Doss, R. (2023). False data injection threats in active distribution systems: A comprehensive survey, *Future Generation Computer Systems* **140**: 344–364, DOI: 10.1016/j.future.2022.10.021.

Jamroen, C. (2022). The effect of SoC management on economic performance for battery energy storage system in providing voltage regulation in distribution networks, *Electric Power Systems Research* **211**: 108340, DOI: 10.1016/j.epsr.2022.108340.

Lei, W., Pang, Z., Wen, H. and Hou, W. (2022). FDI attack detection at the edge of smart grids based on classification of predicted residuals, *IEEE Transactions on Industrial Informatics* **18**(12): 9302–9311.

Li, M., Long, Y., Li, T. and Chen, C. (2022). Consensus of linear multi-agent systems by distributed event-triggered strategy with designable minimum inter-event time, *Information Sciences* **609**: 644–659, DOI: 10.1016/j.ins.2022.07.107.

Li, Y. and Yan, J. (2020). Cybersecurity of smart inverters in the smart grid: A survey, *IEEE Transactions on Power Electronics* **38**(2): 2364–2383.

Liang, G., Weller, S., Zhao, J. and Luo, F. (2016). The 2015 Ukrainian blackout: Implications for false data injection attacks, *IEEE Transactions on Power Systems* **32**(4): 3317–3318.

Liu, C., Ma, X., Zhou, M., Wu, J. and Long, C. (2018). An event-trigger two-stage architecture for voltage control in distribution systems, *International Journal of Electrical Power & Energy Systems* **95**: 577–584, DOI:10.1016/j.ijepes.2017.08.030.

Liu, Y., Wei, Y., Wang, C. and Wu, H. (2024). Trajectory optimization for adaptive deformed wheels to overcome steps using an improved hybrid genetic algorithm and an adaptive particle swarm optimization, *Mathematics* **12**(13): 2077.

Mohan, A., Meskin, N. and Mehrjerdi, H. (2020). A comprehensive review of the cyber-attacks and cyber-security on load frequency control of power systems, *Energies* **13**(15): 3860.

Moudoud, H., Mlika, Z., Khoukhi, L. and Cherkaoui, S. (2022). Detection and prediction of FDI attacks in IoT systems via hidden Markov model, *IEEE Transactions on Network Science and Engineering* **9**(5): 2978–2990.

Murray, W., Adonis, M. and Raji, A. (2021). Voltage control in future electrical distribution networks, *Renewable and Sustainable Energy Reviews* **146**: 111100, DOI: 10.1016/j.rser.2021.111100.

Pang, Z., Fu, Y., Guo, H. and Sun, J. (2023). Analysis of stealthy false data injection attacks against networked control systems: Three case studies, *Journal of Systems Science and Complexity* **36**(4): 1407–1422.

Sarkar, S., Teo, Y. and Chang, E. (2022). A cybersecurity assessment framework for virtual operational technology in power system automation, *Simulation Modelling Practice and Theory* **117**: 102453, DOI: 10.1016/j.simpat.2021.102453.

Shi, J., Yue, D. and Weng, S. (2019). Distributed event-triggered mechanism for secondary voltage control with microgrids, *Transactions of the Institute of Measurement and Control* **41**(6): 1553–1561.

Sun, H., Guo, Q., Qi, J., Ajjarapu, V., Bravo, R., Chow, J. and Yang, G. (2019). Review of challenges and research opportunities for voltage control in smart grids, *IEEE Transactions on Power Systems* **34**(4): 2790–2801.

Sun, H., Huang, J., Chen, Z. and Wang, Z. (2023). State-sensitive event-triggered path following control of autonomous ground vehicles, *Intelligence & Robotics* **3**(3): 257–273.

Xing, Z. and Liu, B. (2022). Vector correlation learning and pairwise optimization feature selection for false data injection attack detection in smart grid, *International Journal of Emerging Electric Power Systems* **23**(6): 831–838.

Yang, H., Deng, C., Xie, X. and Ding, L. (2023). Distributed resilient secondary control for AC microgrid under FDI attacks, *IEEE Transactions on Circuits and Systems II: Express Briefs* **70**(7): 2570–2574.

Zhang, G., Tong, D., Chen, Q. and Zhou, W. (2023). Sliding mode control against false data injection attacks in DC microgrid systems, *IEEE Systems Journal* **17**(4): 6159–6168.

Zhang, X., Han, Q., Ge, X., Ding, D., Ding, L., Yue, D. and Peng, C. (2021). Networked control systems: A survey of trends and techniques, *IEEE/CAA Journal of Automatica Sinica* **7**(1): 1–17.

Zhao, W. (2024). Voltage difference over-limit fault prediction of energy storage battery cluster based on data driven method, *Journal of Intelligent & Fuzzy Systems* **46**(2): 5155–5164.

Zhou, X., Farivar, M., Liu, Z., Chen, L. and Low, S. (2022). Reverse and forward engineering of local voltage control in distribution networks, *IEEE Transactions on Automatic Control* **66**(3): 1116–1128.

Zhu, D., Zhou, Q. and Wang, C. (2022). Research on high-proportion distributed photovoltaic access planning method considering voltage over limit risk, *Journal of Physics: Conference Series* **2399**(1): 012037.

Fang Zhang was born in Ningxia, China, in 1979. She received her BS and MS degrees in electrical engineering from Northeast Electric Power University in 2000 and 2003, respectively, and her PhD degree in electrical engineering from North China Electric Power University in 2016. She has been working at Beijing Information Science & Technology University since 2003, currently as an associate professor. Her present research interests include the analysis and control of power systems with new energy and energy storage.

Received: 25 September 2024
Revised: 16 January 2025
Re-revised: 22 & 23 January 2025
Accepted: 20 February 2025