Received: 2 January 2024 | Revised: 20 April 2024 | Accepted: 29 May 2024

DOI: 10.1002/rnc.7489

RESEARCH ARTICLE

WILEY

Privacy-preserving-based fuzzy filtering for nonlinear networked systems with adaptive-event-triggered mechanism and FDI attacks

Jinliang Liu[1] | **Jiahui Tang**[2] | **Lijuan Zha**[3] | **Xiangpeng Xie**[4] | **Engang Tian**[5] | **Chen Peng**[6]

[1]School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, China

[2]College of Information Engineering, Nanjing University of Finance and Economics, Nanjing, China

[3]College of Science, Nanjing Forestry University, Nanjing, China

[4]Institute of Advanced Technology, Nanjing University of Posts and Telecommunications, Nanjing, China

[5]School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, China

[6]School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China

Correspondence
Jinliang Liu, School of Computer Science, Nanjing University of Information Science and Technology, Nanjing, Jiangsu 210044, China.
Email: liujinliang@vip.163.com

Funding information
National Natural Science Foundation of China, Grant/Award Numbers: 62373252, 62273174; Startup Foundation for Introducing Talent of NUIST, Grant/Award Numbers: 2024r063

Abstract

This article centers around the privacy-preserving-based secure H_∞ filtering issue for interval type-2 (IT-2) fuzzy networked systems with false data injection (FDI) attacks. In order to achieve the goal of privacy preserving and significantly enhancing system security against potential eavesdropping threats, a novel encryption-decryption mechanism (EDM) is adopted to safeguard the safety of signals across the network. The mechanism encrypts the transmitted signal by introducing artificial noise, secret key, and utilizing randomly selected nodes. This ensures that the actual transmitted data remains invisible to eavesdroppers while minimally the impact on the estimated performance of the proposed EDM. Given the network communication resources are becoming constrained due to the ever-increasing network traffic, an adaptive event-triggered mechanism (AETM) is employed to ease network congestion by an adaptively adjustable threshold. Then, various sufficient conditions have been outlined to ensure that the filtering error system meets the prescribed disturbance attenuation level. In the end, a numerical example is presented to evaluate both the precision and effectiveness of the developed algorithms.

KEYWORDS

adaptive event-triggered mechanism, encryption-decryption mechanism, false data injection attacks, interval type-2 fuzzy model, privacy-preserving

1 | INTRODUCTION

Nowadays, the presence of nonlinear elements in physical systems has given rise to substantial challenges for the analysis and synthesis of networked control systems (NCSs). These issues are gathering increasingly more attention in recent years among researchers.[1–3] Particularly, the Takagi–Sugeno (T-S) fuzzy model stands out as one of the most intelligent and efficient methods for the control of nonlinear networked systems since it has the capability to decompose the initial

complex nonlinear systems (NSs) into a composition of multiple subsystems.[4–7] The conventional Interval Type-1 T-S fuzzy model captures system nonlinearities through precise membership functions.[8,9] However, in practical applications, acquiring these precise membership functions for modeling the nonlinear systems can be challenging due to parameter uncertainties. By comparison, the Interval Type-2 (IT-2) T-S fuzzy model can effectively meet this requirement by utilizing lower and upper membership functions. Emphasizing the merits of IT-2 fuzzy model, a multitude of outcomes have been widely reported.[10–13] To name a few, in Reference 12, an adaptive IT-2 fuzzy event-triggered control method was introduced to optimize tracking for uncertain cyclic switched stochastic NSs. In Reference 13, it focused on the security control issue for nonlinear networked systems built upon an IT-2 T-S fuzzy dynamics by employing a fuzzy observer. Therefore, it is clear that the IT-2 T-S fuzzy approach is indeed an effective strategy for dealing with NSs.

With the significant focus directed toward NCSs, there has been a notable surge of interest in tackling the challenge of filtering problems within NCSs. Until now, considerable literatures have yielded substantial and valuable findings on this particular issue.[14–21] For instance, Li et al.[15] proposed a resilient unscented Kalman filter to handle the fusion estimation problem of multiple unmanned aerial vehicles. However, such Kalman filters are always based on the premise that external spectral noise densities are accessible beforehand to minimize filtering errors. Consequently, H_∞ filtering methods emerge as a viable solution to address system uncertainties. The widespread adoption of the H_∞ filter in practical engineering is attributed to its ability to offer robustness against worst-case estimation errors without necessitating prior knowledge of noise statistics. The authors in Reference 16 addressed a resilient H_∞ secure state estimation issue to resist gain variations and stochastic disturbances. A novel distributed H_∞ filter model was applied for switched stochastic time-delayed networked systems subject to randomly occurring fading measurements in Reference 17. Hence, it is reasonable to adopt H_∞ filtering approaches to estimate the system value and recover the true signals within NCSs.

At the same time, the constraints of network bandwidth, coupled with the explosive growth of data in the plant, are frontier issues in research. In an effort to conserve the limited network bandwidth and alleviate network congestion, there has been a significant surge in the exploration of various event-triggered schemes in recent years. In the early stage, time-triggered strategies, where the sampled data was transmitted at fixed time intervals, were widely employed. However, such a mechanism may result in excessive data transmission as the system approaches stability. Thus, a static event-triggered mechanism (SETM) was proposed to decrease unnecessary transmission,[22–24] in which the transmission of data depended on a predefined threshold. Subsequently, some scholars have also conducted research on new event-triggered mechanisms, including memory event-triggered fault detection,[25] event-triggered differential tracking control,[26] and memory-based continuous event-triggered control.[27] At present, the concept of adaptive event-triggered mechanism (AETM) has been introduced, where the triggered threshold is adaptively adjustable at intervals by the varying signals, resulting in multiple outcomes.[28–32] To highlight a few specific examples, the authors in Reference 29 adopted an AETM to realize the distributed synchronization for NCSs with actuator bias faults. In Reference 30, it focused on neural-network-based control for uncertain NSs in the presence of AETM. Inspired by the results before, this paper will utilize the AETM to mitigate the challenges posed by limited bandwidth.

In addition to the challenges posed by restricted bandwidth in wireless communication networks, another critical area of concern for NCSs lies in the field of network security. Given the openness and inherent vulnerabilities of communication networks, NCSs are highly susceptible to potential cyber attacks. Consequently, these vulnerabilities pose significant challenges for tasks such as system state estimation and control. At present, many researchers are concentrating their efforts on this hot topic and numerous valuable achievements have been put forth.[33–36] There are primarily three categories of cyber attacks, namely deception attacks,[37,38] denial-of-service (DoS) attacks[39,40] and replay attacks.[41,42] Typically, false data injection (FDI) attacks are one type of deception attacks, which have the potential to severely impact system performance by tampering with the original data packets. In Reference 37, the event-triggered control problem was addressed for the semi-Markovian switching systems against FDI attacks. Chen et al.[36] took the FDI attacks on actuators into consideration, and then proposed an attack-tolerant control strategy.

On the other hand, as information technology advances, the exponential growth of data results in a continual expansion of information volume. The issue of information leakage in NCSs is inevitable, compounded by the growing concern for privacy preservation by individuals. The potential eavesdroppers might infer the private information of the system by overhearing the transmitted signals over communication networks. There is no doubt that the phenomenon of information leakage poses serious threats to so-called information security and may lead to severe losses. In the existing studies, significant attention has been directed toward the issue of privacy preserving, among which one possible solution is the encryption-decryption mechanism (EDM), and fruitful outcomes have been available now.[43–49] The authors in Reference 44 focused on the edge-event-trigger control for multi-agent systems based on an observer. In Reference 45, Li et al.

presented a novel detection algorithm for replay attacks by adopting a dynamic EDM. The authors in Reference 49 proposed a novel EDM based on state decomposition with added noises. Given the practical challenges at hand, it makes sense to give due consideration to the concerns surrounding network security and privacy preserving.

In light of the aforementioned discussions, this article focuses on the privacy-preserving-based H_∞ filtering issue for IT-2 fuzzy networked systems. To alleviate the phenomenon of constrained network bandwidth, an AETM has been implemented. However, during the transmission of signals through communication networks, the occurrence of FDI attacks cannot be overlooked, as they can do serious harm to the system. Besides, a novel EDM has been proposed for the sake of privacy preserving. To the best of our knowledge, none of the existing publications draw attention to such a topic, which motivates us to carry out relevant research. All in all, the central novelties can be listed as follows:

1. The IT-2 fuzzy networked system dynamics incorporates considerations for randomly occurring FDI attacks, which may pose a serious threat to system integrity, availability, and confidentiality. To manage the constraints of limited network bandwidth effectively, an AETM is employed to mitigate communication load by utilizing an adaptively adjustable threshold. Compared to the normal SETM in References 22–24, AETM allows for flexible event triggering instants based on conditions, offering greater adaptability and scalability.
2. A novel EDM is put forward to deal with potential eavesdropping attacks for the purpose of privacy preserving. Compared with existing works such as References 44 and 50, the proposed algorithm not only encrypts the transmitted signal with a secret key but also incorporates randomly selected encryption nodes and artificial noise. This integration improves the randomness of decryption, effectively addressing concerns related to key theft, which ensures the system's estimation performance while enhancing its security capabilities.
3. Sufficient conditions are derived to address the fuzzy filtering error system in the presence of the AETM, EDM, and FDI attacks, aiming to maintain a desirable disturbance attenuation level. Considering these factors, the time-varying fuzzy filter gains are calculated by the solvable sufficient conditions.

Here is the structure of our work. In Section 2, the framework of fuzzy dynamics, along with AETM and EDM based communication scheme is established. In Section 3, the EDM algorithm is designed and time-varying filter gains are obtained. To validate the efficacy of the AETM and EDM algorithm, as well as the filtering performance, a numeric example is presented in Section 4. Ultimately, some conclusions along with future work directions are derived in Section 5.

Notations: The notations used in this article are standard. Additionally, 1_p denotes a $p \times 1$ column vector with all elements equal to 1. $\lambda_{\max}(A)$ means the maximum eigenvalue of A. $\delta(A)$ means the Kronecker delta function. $diag\{\dots\}$ represents the block-diagonal matrix.

2 | PROBLEM FORMULATION

2.1 | System model and AETM

This article focuses on the secure fuzzy filtering issue for discrete-time nonlinear NCSs. An IT-2 fuzzy system with h rules is modeled in the following form:

Rule g **: IF** $\varpi_1(x(k))$ is Z_1^g, $\varpi_2(x(k))$ is Z_2^g, $\dots$, $\varpi_d(x(k))$ is Z_d^g, **THEN**

$$\begin{cases} x(k+1) &= \sum_{g=1}^{h} \theta_g(x(k))\left[A_g(k)x(k) + B_g(k)\omega(k)\right], \\ y(k) &= C(k)x(k) + D(k)\omega(k), \\ z(k) &= \sum_{g=1}^{h} \theta_g(x(k))M_g(k)x(k), \end{cases} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$, $\omega(k) \in \mathbb{L}_2[0,\infty)$, $y(k) \in \mathbb{R}^t$, $z(k) \in \mathbb{R}^{n_z}$ represent the state vector, the disturbance input, the measurement output and the signal to be estimated, respectively. $A_g(k), B_g(k), C(k), D(k), M_g(k)$ are known time-varying matrices with appropriate dimensions.

As to fuzzy parameters, $\theta_g(x(k)) = \frac{b_g(x(k))}{\sum_{g=1}^{h} b_g(x(k))}$, $b_g(x(k)) = \underline{\theta}_g(x(k))\underline{o}_g(x(k)) + \overline{\theta}_g(x(k))\bar{o}_g(x(k)) \cdot \underline{o}_g(x(k)), \bar{o}_g(x(k)) \in [0,1]$ stand for nonlinear weighting functions that satisfy $\underline{o}_g(x(k)) + \bar{o}_g(x(k)) = 1$. Z_q^g $(q = 1, 2, \ldots, d, g = 1, 2, \ldots, h)$ denotes the gth fuzzy sets. $\varpi_q(x(k))$ is the premise variable. The membership value $\theta_g(x(k))$ satisfies $\sum_{g=1}^{h}\theta_g(x(k)) = 1$. Set the gth firing strength as:

$$\iota_g(x(k)) = [\underline{\theta}_g(x(k)), \overline{\theta}_g(x(k))], \tag{2}$$

where $\underline{\theta}_g(x(k)) = \prod_{i=1}^{d}\underline{Z}_i^g(\varpi_i(x(k))) \geq 0, \overline{\theta}_g(x(k)) = \prod_{i=1}^{d}\overline{Z}_i^g(\varpi_i(x(k)) \geq 0$ with the lower and upper membership functions satisfying $0 \leq \underline{Z}_i^g(\varpi_i(x(k))) \leq \overline{Z}_i^g(\varpi_i(x(k)) \leq 1$.

In the collaborative communication channel connecting sensors and filters, constrained network resources often lead to unwelcome occurrences, notably data conflicts and network congestion. Our primary concern is effectively mitigating these issues to ensure seamless and dependable data transmission.

To address unnecessary data transfer and optimize communication resources, an AETM is employed. This mechanism ensures the transfer of measured signals at each sampling instant, effectively overcoming the constraints imposed by limited resources. For simplicity, the event triggered sequences are expressed as $\mathbb{T} = \{t_n | n = 0, 1, 2, \ldots\}$. Thus, the adopted AETM can be described as

$$\sigma y^T(k)y(k) - \Delta^T(k)\Delta(k) + \frac{1}{\chi}\epsilon(k) < 0, \tag{3}$$

where $\Delta(k) = y(k) - y(t_n)(k \in [t_n, t_{n+1}))$ refers to the gap between current sampling signal $y(k)$ and most recent triggered signal $y(t_n)$. χ is a given positive scalar and $\sigma \in (0,1)$ is called AETM parameter. The variable $\epsilon(k)$ represents the adaptive threshold, and it is computed as

$$\begin{cases} \epsilon(k+1) = \sigma y^T(k)y(k) - \Delta^T(k)\Delta(k) + \lambda\epsilon(k), \\ \epsilon(0) = \epsilon_0, \end{cases} \tag{4}$$

where ϵ_0 is a prescribed initial condition.

Additionally, the signal can be transmitted if (3) is satisfied. Therefore, one can come to the event triggered instants that

$$t_{n+1} = \inf_{k \geq t_n}\{k | k > t_n, \text{satisfying(3)}\}. \tag{5}$$

Remark 1. In case the condition specified in (3) is met during data transmission, the sensor will release the timely measurable signal $y(t_n)$ into the communication network. In other words, the measurement output can be transmitted only when the applied AETM condition is fulfilled. Additionally, it is worth noting that as $\chi \to \infty$, AETM will transition into a SETM.

As data packages can only be sent to the communication network during triggered instants, time instants that violate the triggered conditions will have nothing to transfer. Consequently, a zero-order holder (ZOH) technique is selected for adoption. Hence, the updating standards are denoted in the following form:

$$\bar{y}(k) = \begin{cases} y(t_n), & \text{if (3) is satisfied,} \\ \bar{y}(k-1), & \text{otherwise.} \end{cases} \tag{6}$$

From (5) and (6), one can get that

$$t_n = \begin{cases} k, & \text{if (3) is satisfied,} \\ t_{n-1}, & \text{otherwise.} \end{cases} \tag{7}$$

To distinguish between various time instants, the Kronecker delta function $\delta(k - t_n) \in \{0, 1\}$ is applied to signify whether a time instant is triggered or not. For simplicity, we denote $\delta(k - t_n)$ as β_k, whereby it can be effortlessly

obtained that

$$\bar{y}(k) = \beta_k y(t_n) + (1 - \beta_k)\bar{y}(k-1). \tag{8}$$

2.2 | Encryption and decryption mechanism

Encryption scheme: For all k, set the ciphertext $\bar{y}(k)$ through the following derivation:

$$\bar{y}(k) = \begin{cases} y(t_n) + S\Phi(\pi_k)\zeta(k), & \text{if (3) is satisfied ,} \\ \bar{y}(k-1), & \text{otherwise,} \end{cases} \tag{9}$$

where the orthogonal matrix $S \in \mathbb{R}^{t\times t}$ represents the secret key. $\pi_k \in U = \{1, 2, \dots, t\}$ is referred to as the randomly chosen encrypted nodes, which aligns with the probability distribution $Prob\{\pi_k = m\} = p_m, m \in U$. $\Phi(\pi_k) = diag\{\delta(1 - \pi_k), \delta(2 - \pi_k), \dots, \delta(t - \pi_k)\}$ indicates the nodes selection status. $\zeta(k)$ symbolizes a human-made noise vector.

Remark 2. Currently, privacy preserving has become a hot topic of research, reflecting the growing concern over data security breaches. The primary method employed to achieve these privacy objectives is EDM, which utilizes secret-key-based encryption to safeguard transmitted data. In practical applications, the secret key S is exclusively accessible to the filter side and remains concealed from other units. This ensures that the real signals transmitted through the network are disguised, making it difficult for eavesdroppers to intercept and decipher the information. As a result, the security performance of the system is enhanced.

Remark 3. Compared with Reference 50, the EDM presented in this paper possesses greater flexibility and security. In Reference 50, the secret key S was defined as a nonzero matrix. The encryptor was set as $\bar{y}(k) = y(k) + S$ and the decryptor was followed by $\hat{y}(k) = \bar{y}(k) - S$. However, such a method becomes vulnerable once the key is obtained by the eavesdroppers, rendering it ineffective. Thus, it is worth noting that the random selection of encryption nodes and the inclusion of artificial noise can significantly enhance system security against eavesdropping threats, while minimizing the impact on state estimation performance. On account of the randomness of the encryption nodes, it becomes practically infeasible to retrieve the original signal during decryption by simply subtracting the encryption items. In addition, the introduction of artificial noise vectors has a notable impact on eavesdroppers. Under such a mechanism, even if the eavesdroppers manage to acquire the secret key, they still cannot decrypt the original data. This substantial improvement in security greatly fortifies the overall system performance.

The encrypted signals are highly susceptible to randomly occurring injection attacks during transmission across the communication network due to inherent openness of NCSs, which have the potential to compromise the integrity of the transmitted signals. However, in real-world scenarios, attackers face challenges in sustaining a consistent emission of attack signals due to various constraints, such as energy limitations. Hence, variable $\alpha(k)$ follows a Bernoulli distribution. $E\{\alpha(k)\} = \bar{\alpha} \in [0, 1]$ is employed to describe malicious false data injection attacks that occur randomly and exclusively impact the transmitted signals. $\bar{\alpha}$ is a prescribed scalar.

Denote $\check{y}(t_n) = y(t_n) + S\Phi(\pi_k)\zeta(k)$. Then taking the influence of FDI attacks into account, the transmitted sequences in (9) are reformulated as

$$\bar{y}(k) = \begin{cases} \check{y}(t_n) + \alpha(k)v(k), & \text{if (3) is satisfied ,} \\ \bar{y}(k-1), & \text{otherwise,} \end{cases} \tag{10}$$

where $v(k)$ represents false data signal which is correlated with $x(k)$. Given a matrix $\mathcal{G}$ with suitable dimension, $v(k)$ satisfies the following condition:

$$v^T(k)v(k) \le x^T(k)\mathcal{G}^T\mathcal{G}x(k). \tag{11}$$

Remark 4. It is reasonable to employ a stochastic method to model FDI attacks and to consider the constraint outlined in (11). Such results are presented in some existing literatures.[3,51] In Reference 3, the authors consider

the outlier-resistant quantized control issue under randomly occurring network attacks with a given probability. In Reference 51, the authors put forward a partial FDI attack method which can inject false signals into the feedback communication channel with specific probabilities to manipulate certain sensor measurements. From the viewpoint of defenders, it makes sense to get the probability distribution of attacks to improve the security and reliability when designing the desired filters and such method is often adopted to describe the FDI attacks.

For the convenience in the design of EDM, the transmitted signal at triggered instant k is represented as

$$\tilde{y}(k) = C(k)x(k) + D(k)w(k) + \alpha(k)v(k) + S\Phi(\pi_k)\zeta(k). \tag{12}$$

Moreover, the overall received measurement $\bar{y}(k)$ at the filter side is concluded to be

$$\begin{aligned}\bar{y}(k) =&\beta_k[y(t_n) + S\Phi(\pi_k)\zeta(k) + \alpha(k)v(k)] + (1-\beta_k)\bar{y}(k-1)\\ =&\beta_k[C(k)x(k) + D(k)w(k) - \Delta(k) + S\Phi(\pi_k)\zeta(k) + \alpha(k)v(k)] + (1-\beta_k)\bar{y}(k-1).\end{aligned} \tag{13}$$

After the transmission of encrypted signal $\bar{y}(k)$ through the network, the following decryption mechanism is adopted to transform the ciphertext into plaintext.

Decryption scheme: The decrypted measurement signal can be obtained through the following process:

$$\begin{cases}\tilde{\pi}_k = \underset{m}{argmin}\Psi_k(\Phi(m)),\\ \hat{y}(k) = S(I - \Phi(\tilde{\pi}_k))S^T\bar{y}(k),\end{cases} \tag{14}$$

where $\tilde{\pi}_k$ represents the estimated node π_k, and it's crucial that they should match π_k selected at random during the encryption phase. $\hat{y}(k)$ refers to the decrypted measurement signal after transmitting through the communication network and $\Psi_k(\Phi(m))$ stands for the decryption function to be obtained later.

Remark 5. EDM is popularly employed to tackle secure state estimation issues and effectively counteract the risks posed by eavesdropping. The advantages of introducing AETM when designing privacy protection solutions can be listed as: (1) The EDM in this article involves some auxiliary parameters and will add extra computational complexities, imposing significant communication burden on limited bandwidth. Therefore, AETM is adopted to alleviate the communication load caused by EDM, and compared to traditional SETM, AETM can transmit fewer data packets. (2) As the decryption function design incorporates the system state at previous moments, not just the triggered instants. Eavesdroppers can only access transmitted signals at these triggered instants, and they are unable to retrieve the original signal, thereby enhancing the security performance of encryption and decryption algorithms.

2.3 | Fuzzy filter design and system augmentation

To tackle the inherent challenge of dealing with the factors mentioned above, the proposed fuzzy filter structure with h rules has been structured in the following manner:

Rule r **: IF** $\varpi_1(\hat{x}(k))$ is Z_1^r, $\varpi_2(\hat{x}(k))$ is Z_2^r, … , $\varpi_d(\hat{x}(k))$ is Z_d^r, **THEN**

$$\begin{cases}\hat{x}(k+1) &= \sum_{r=1}^{h}\theta_r(x(k))[A_r(k)\hat{x}(k) + K_{r,\tilde{\pi}_k}(k)(\hat{y}(k) - \tilde{\Phi}(\tilde{\pi}_k)C(k)\hat{x}(k))],\\ \hat{z}(k) &= \sum_{r=1}^{h}\theta_r(x(k))M_r(k)\hat{x}(k),\end{cases} \tag{15}$$

where $\hat{x}(k)$, $\hat{z}(k)$ refer to the estimation of $x(k)$ and the estimated signal $z(k)$. $K_{r,k}(\tilde{\pi}_k)$ stands for the time-varying filter gains acquired from encrypted nodes. Denote $\tilde{\Phi}(\tilde{\pi}_k) = S(I - \Phi(\tilde{\pi}_k))S^T$.

By using the properties of $\Phi(\tilde{\pi}_k)$ and S, it is obvious that $\tilde{\Phi}(\tilde{\pi}_k)S\Phi(\pi_k)\zeta(k) = S(I-\Phi(\tilde{\pi}_k))S^TS\Phi(\pi_k)\zeta(k) = 0$, then define $e(k) = x(k) - \hat{x}(k)$, and substitute (13), (14) into (15), one has

$$\begin{cases} \hat{x}(k+1) = \sum_{r=1}^{h}\theta_r(\hat{x}(k))[(A_r(k)(x(k)-e(k)) + \beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)C(k)x(k) \\ \quad +\beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)D(k)w(k) + \beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)\alpha(k)v(k) \\ \quad -\beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)\Delta(k) + (1-\beta_k)K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)\bar{y}(k-1) \\ \quad -K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)(x(k)-e(k))], \\ \tilde{z}(k) = \sum_{r=1}^{h}\theta_r(\hat{x}(k))M_r(k)(x(k)-e(k)). \end{cases} \tag{16}$$

Therefore, setting $\tilde{z}(k) = z(k) - \hat{z}(k)$, the fuzzy filtering error system resulting from (1) and (16) is characterized as

$$\begin{cases} e(k+1) = \sum_{g=1}^{h}\sum_{r=1}^{h}\theta_g(x(k))\theta_r(\hat{x}(k))[(A_g(k) - A_r(k) - (\beta_k-1)K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)C(k))x(k) \\ \quad +(A_r(k) - K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)C(k))e(k) + (B_g(k) - \beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)D(k))w(k) \\ \quad -\beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)\alpha(k)v(k) + \beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)\Delta(k) \\ \quad -(1-\beta_k)K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)\bar{y}(k-1)], \\ \tilde{z}(k) = \sum_{g=1}^{h}\sum_{r=1}^{h}\theta_g(x(k))\theta_r(\hat{x}(k))(M_g(k) - M_r(k))x(k) + M_r(k)e(k). \end{cases} \tag{17}$$

Let $\xi(k) = [x^T(k) \quad e^T(k) \quad \bar{y}^T(k-1)]^T$, then the augmented filtering error system is reformulated as

$$\begin{cases} \xi(k+1) = \sum_{g=1}^{h}\sum_{r=1}^{h}\theta_g(x(k))\theta_r(\hat{x}(k))[\bar{A}_{g,r,\tilde{\pi}_k}\xi(k) + (\alpha(k)-\overline{\alpha})\overline{B}_{r,\tilde{\pi}_k}v(k) + \overline{\alpha}\overline{B}_{r,\tilde{\pi}_k}v(k) \\ \quad +\overline{D}_{g,r,\tilde{\pi}_k}w(k) + \bar{E}_{r,\tilde{\pi}_k}\Delta(k)], \\ \tilde{z}(k) = \sum_{g=1}^{h}\sum_{r=1}^{h}\theta_g(x(k))\theta_r(\hat{x}(k))\overline{M}_{g,r}\xi(k), \end{cases} \tag{18}$$

where

$$\bar{A}_{g,r,\tilde{\pi}_k} = \begin{bmatrix} A_g(k) & 0 & 0 \\ a_{21} & a_{22} & a_{23} \\ a_{31} & 0 & 1-\beta_k \end{bmatrix}, \overline{B}^T_{r,\tilde{\pi}_k} = \begin{bmatrix} 0 & b^T_{21} & b^T_{31} \end{bmatrix}^T, \bar{E}^T_{r,\tilde{\pi}_k} = \begin{bmatrix} 0 & e^T_{21} & e^T_{31} \end{bmatrix}^T, \overline{D}^T_{g,r,\tilde{\pi}_k} = \begin{bmatrix} B_g(k) & d^T_{21} & d^T_{31} \end{bmatrix}^T,$$

$$\overline{M}_{g,r} = \begin{bmatrix} M_g(k) - M_r(k) & M_r(k) & 0 \end{bmatrix}, a_{21} = A_g(k) - A_r(k) - (\beta_k-1)K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)C(k),$$

$$a_{22} = A_r(k) - K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)C(k), a_{23} = (\beta_k-1)K_{r,\tilde{\pi}_k}(k), a_{31} = \beta_k\tilde{\Phi}(\tilde{\pi}_k)C(k),$$

$$b_{21} = -\beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k), b_{31} = \beta_k\tilde{\Phi}(\tilde{\pi}_k), d_{21} = B_g(k) - \beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)D(k), d_{31} = \beta_k\tilde{\Phi}(\tilde{\pi}_k)D(k),$$

$$e_{21} = \beta_k K_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k), e_{31} = -\beta_k\tilde{\Phi}(\tilde{\pi}_k).$$

Here, we will present the main purpose of this article:

(1) Design the decryption function $\Psi_k(\Phi(m))$ and human-made noise vector $\zeta(k)$, then the secret capacity $\mathcal{S}_k > \tau$ holds for all k.

(2) Design the time-varying fuzzy filter gains $K_{r,\tilde{\pi}_k}(k)$ such that the following H_∞ performance can be met:

$$E\left\{\sum_{k=0}^{\infty}\left\|\tilde{z}(k)^2\right\|\right\}-\gamma^2\sum_{k=0}^{\infty}\|\omega(k)\|^2\leq 0,$$

where γ is the H_∞ disturbance attenuation level.

In the upcoming section, some foundational concepts that are crucial for establishing the primary outcomes will be presented.

Definition 1 (52). For the given matrices $A_g(k)(g=1,2,\ldots,h)$ and $C(k)$, the matrix pairs $(A_g(k),C(k))$ are called uniformly observable if there exists a positive scalar ε and an integer $\tilde{N}$ satisfying the restrictions $\sum_{t=k}^{k+\tilde{N}}\overline{\mathcal{A}}_t^T(k)C^T(k)C(k)\overline{\mathcal{A}}_t(k)\geq\varepsilon I$, where

$$\bar{A}_t(k)=\begin{cases}\sum_{g=1}^{h}\theta_g(k)A_g(k)\ \ldots\ \theta_g(t-2)A_g(t-2)\theta_g(t-1)A_g(t-1), & if\ t>k,\\ I, & if\ t=k.\end{cases}$$

Definition 2 (13). For the give scalar $\gamma>0$, the H_∞ performance index of the augment fuzzy system is met if the given equality holds:

$$E\left\{\sum_{k=0}^{\infty}\left\|\tilde{z}(k)^2\right\|\right\}-\gamma^2\sum_{k=0}^{\infty}\|\omega(k)\|^2\leq 0.$$

Assumption 1. The inequalities $\tilde{\mathcal{C}}_m^T(k)\tilde{\mathcal{C}}_m(k)\geq\kappa C^T(k)\ C(k)$ hold, where $\tilde{\mathcal{C}}_m(k)=(I-\Phi(m))S^TC(k)$. κ is a predesigned positive scalar.

Assumption 2. The norms of initial state vector $x(0)$, time-varying disturbances $w(k)$ and the false data injection signal $v(k)$ exhibit the upper bounds as listed:

$$\|x(0)\|\leq\epsilon_0,\|w(k)\|\leq w_0,\|v(k)\|\leq v_0,$$

where ϵ_0,w_0,v_0 are predefined positive constants.

3 | MAIN RESULTS

In this context, we will discuss the design of the decryption function $\Psi_k(\Phi(m))$ aimed at significantly reducing the influence of $\zeta(k)$ throughout the estimation process. Meanwhile, indicators for evaluating the overall security capability will be proposed. Furthermore, an analysis will be carried out to assess the H_∞ index of the suggested augmented model and the corresponding filter parameters are to be calculated.

In Theorem 1, it will be demonstrated the ciphertext $\tilde{y}(k)$ at triggered instants can be used to assess the impact brought by external inputs. This contributes to the design of $\Psi_k(\Phi(m))$.

Theorem 1. *Taking the aforementioned assumptions and the fuzzy system (1) into consideration, the ciphertext sequences at triggered instant k are represented as*

$$\begin{cases}\mathcal{H}_{\tilde{\hbar}}(\Phi(m))=\mathcal{P}_{\tilde{\hbar}}(\Phi(m)), & if\ k\geq\tilde{N},\\ \tilde{\Phi}(m)\tilde{y}(\tilde{\hbar})=\tilde{\Phi}(m)\vec{o}(\tilde{\hbar}), & if\ k<\tilde{N},\end{cases}\tag{19}$$

where

$$k-\tilde{N}=\jmath, k+1=\tilde{\hbar}, s(k)=S\Phi(\pi_k)\zeta(k), \overline{\Phi}(m)=(I-\Phi(m))S^T,$$

$$\Omega(k)=\begin{bmatrix}\tilde{\mathcal{C}}_{\pi_\jmath}(\jmath)\\ \tilde{\mathcal{C}}_{\pi_{\jmath+1}}(\jmath+1)\overline{\mathcal{A}}_{\jmath+1}(\jmath)\\ \vdots\\ \tilde{\mathcal{C}}_{\pi_k}(k)\overline{\mathcal{A}}_k(\jmath)\end{bmatrix}, \mathcal{Q}^m_{r,\tilde{\hbar}}=\tilde{\mathcal{C}}_m(\tilde{\hbar})\overline{\mathcal{A}}_{\tilde{\hbar}}(\jmath)(\Omega^T(k)\Omega(k))^{-1}\tilde{\mathcal{C}}_{\pi_{\jmath+r}}(\jmath+1)\overline{\mathcal{A}}_{\jmath+r}(\jmath),$$

$$\mathcal{Q}^m_{\tilde{\hbar}}=\left[\mathcal{Q}^m_{0,\tilde{\hbar}},\ \mathcal{Q}^m_{1,\tilde{\hbar}},\ \dots,\ \mathcal{Q}^m_{\tilde{N},\tilde{\hbar}}\right]=\tilde{\mathcal{C}}_m(\tilde{\hbar})\overline{\mathcal{A}}_{\tilde{\hbar}}(\jmath)(\Omega^T(k)\Omega(k))^{-1}\Omega^T(k),$$

$$\lambda(p)=C(p)\sum_{q=\jmath}^{p-1}\overline{\mathcal{A}}_{p-1}(q)B_g(q)w(q), \tilde{o}(q)=D(q)w(q)+s(q)+\alpha(q)v(q)+\lambda(q),$$

$$\vec{o}(q)=C(q)\overline{\mathcal{A}}_q(0)x(0)+C(q)\sum_{j=0}^{q-1}\overline{\mathcal{A}}_{q-1}(j)B_g(j)w(j)+D(q)w(q)+s(q),$$

$$\mathcal{H}_{\tilde{\hbar}}(\Phi(m))=\overline{\Phi}(m)\tilde{y}(\tilde{\hbar})-\sum_{u=0}^{\tilde{N}}\mathcal{Q}^m_{r,\tilde{\hbar}}\overline{\Phi}(\pi_{\jmath+u})\tilde{y}(\jmath+u), \mathcal{P}_{\tilde{\hbar}}(\Phi(m))=\overline{\Phi}(m)\tilde{o}(\tilde{\hbar})-\sum_{u=0}^{\tilde{N}}\mathcal{Q}^m_{r,\tilde{\hbar}}\overline{\Phi}(\pi_{\jmath+u})\tilde{o}(\jmath+u).$$

Proof. Based on the specific values of k, the demonstration can be separated into two distinct segments.

Case I $\{k<\tilde{N}\}$: By using the iterative method to (1), one has

$$x(\tilde{\hbar})=\overline{\mathcal{A}}_{\tilde{\hbar}}(0)\epsilon_0+\sum_{j=0}^{k}\overline{\mathcal{A}}_k(j)B_g(j)w(j). \tag{20}$$

Substituting (20) into $\tilde{y}(\tilde{\hbar})$, it's not difficult to maintain

$$\begin{aligned}\tilde{y}(\tilde{\hbar})=&C(\tilde{\hbar})[\overline{\mathcal{A}}_{\tilde{\hbar}}(0)x(0)+\sum_{j=0}^{k}\overline{\mathcal{A}}_k(j)B_g(j)w(j)]+D(\tilde{\hbar})w(\tilde{\hbar})+\alpha(\tilde{\hbar})v(\tilde{\hbar})+s(\tilde{\hbar})\\ =&\vec{o}(\tilde{\hbar}),\end{aligned} \tag{21}$$

Case II $\{k\geq\tilde{N}\}$: From Assumption 1 and the definition of $\Omega(k)$, the following equalities hold:

$$\begin{aligned}\Omega^T(k)\Omega(k)=&\sum_{q=\jmath}^{k}\overline{\mathcal{A}}^T_q(\jmath)\tilde{\mathcal{C}}^T_{\pi_q}(q)\tilde{\mathcal{C}}_{\pi_q}(q)\overline{\mathcal{A}}_q(\jmath)\\ \geq&\kappa\sum_{q=\jmath}^{k}\overline{\mathcal{A}}^T_q(\jmath)C^T(q)C(q)\overline{\mathcal{A}}_q(\jmath)\\ \geq&\kappa\varepsilon I,\end{aligned} \tag{22}$$

from which one can come to the conclusion that $\Omega^T(k)\Omega(k)$ is invertible.

By employing iterative algorithm on $\overline{y}(k)$, it is evident that

$$\tilde{y}(\jmath+f)-D(\jmath+f)w(\jmath+f)-\alpha(\jmath+f)v(\jmath+f)-s(\jmath+f)=C(\jmath+f)\bar{A}_{\jmath+f}(\jmath)x(\jmath)+\lambda(\jmath+f). \tag{23}$$

Then post-multiplying $\mathcal{Q}^m_{\tilde{\hbar}}$ by $\Omega(k)x(\jmath)$, one has $\mathcal{Q}^m_{\tilde{\hbar}}\Omega(k)x(\jmath)=\tilde{\mathcal{C}}_m(\tilde{\hbar})\overline{\mathcal{A}}_{\tilde{\hbar}}(\jmath)x(\jmath)$, which implies that

$$\overline{\Phi}(m)C(\tilde{\hbar})\overline{\mathcal{A}}_{\jmath+p}(\jmath)x(\jmath)=\overline{\Phi}(m)(\tilde{y}(\tilde{\hbar})-D(\tilde{\hbar})w(\tilde{\hbar})-\alpha(\tilde{\hbar})v(\tilde{\hbar})-s(\tilde{\hbar})-\lambda(\tilde{\hbar})) \tag{24}$$

and

$$\sum_{f=0}^{\tilde{N}} \mathcal{Q}_{f,\tilde{\hbar}}^{m} \tilde{C}_{\pi_{\jmath+f}}(\jmath+f)\overline{\mathcal{A}}_{\jmath+f}(\jmath)x(\jmath)$$
$$=\sum_{f=0}^{\tilde{N}} \mathcal{Q}_{f,\tilde{\hbar}}^{m} \overline{\Phi}(\pi_{\jmath+f})(\tilde{y}(\jmath+f)-D(\jmath+f)w(\jmath+f)-\alpha(\jmath+f)v(\jmath+f)-s(\jmath+f)-\lambda(\jmath+f)). \tag{25}$$

Therefore, on the basis of (23)–(25), the following equality can be simply formulated:

$$\overline{\Phi}(m)(\tilde{y}(\tilde{\hbar})-D(\tilde{\hbar})w(\tilde{\hbar})-\alpha(\tilde{\hbar})v(\tilde{\hbar})-s(\tilde{\hbar})-\lambda(\tilde{\hbar}))$$
$$=\sum_{f=0}^{\tilde{N}} \mathcal{Q}_{f,\tilde{\hbar}}^{m} \overline{\Phi}(\pi_{\jmath+f})(\tilde{y}(\jmath+f)-D(\jmath+f)w(\jmath+f)-\alpha(\jmath+f)v(\jmath+f)-s(\jmath+f)-\lambda(\jmath+f)). \tag{26}$$

Accordingly, it can be concluded that $\mathcal{H}_{\tilde{\hbar}}(\Phi(m)) = \mathcal{P}_{\tilde{\hbar}}(\Phi(m))$ holds for all $m \in \{1, 2, \ldots, t\}$ in Case II. Then the demonstration is finished. ∎

According to Theorem 1, the alignment of the encrypted nodes π_k with corresponding decrypted nodes $\tilde{\pi}_k$, as well as the formulation of the decryption function $\Psi_k(\Phi(m))$, will be considered in Theorem 2.

Theorem 2. *The decryption function is designed as* $\Psi_k(\Phi(m)) \triangleq \begin{cases} \mathcal{H}_k(\Phi(m)), \text{if } k \geq \tilde{N}+1 \\ \overline{\Phi}(m)\bar{y}(k), \text{if } k < \tilde{N}+1 \end{cases}$, *then* $\tilde{\pi}_k = \pi_k$ *holds* $\forall m \in U$ *if* $|\zeta_m(k)| > \max\{\vec{\zeta}, \tilde{\zeta}\}$ *for all* $k \geq 0$, *where*

$$a = \max\left\{\sum_{g=1}^{h}\theta_g(k)A_g(k)\right\}, c = \max\{C(k)\}, b = \max\left\{\sum_{g=1}^{h}\theta_g(k)B_g(k)\right\}, d = \max\{D(k)\},$$
$$\varpi_q = c\sum_{p=0}^{q-1}a^p b w_0 + v_0 + d w_0, \vec{\zeta} = 2\left(\varpi_{\tilde{N}+1} + \sum_{p=0}^{\tilde{N}}\frac{c^2 a^{\tilde{N}+j+1}}{\kappa\varepsilon}\varpi_p\right), \tilde{\zeta} = 2(c\epsilon_0 + \varpi_{\tilde{N}}).$$

Proof. Next, we will consider the norms of $\mathcal{P}_{\tilde{\hbar}}(\Phi(m))$ and $\Phi(m)\vec{o}(p)$ in four distinct scenarios separately.

To begin with, on the basis of the properties of $\Phi(m)$ and secret key S, it poses no difficulty for us to obtain $\|\Phi(m)\| \leq 1$, $\left\|\mathcal{Q}_{q,k+1}^{m}\right\| \leq \frac{c^2 a^{\tilde{N}+q+1}}{\kappa\varepsilon}$, $\|\lambda(q)\| \leq c\sum_{p=0}^{q-1}a^p b w_0$ $(q = 0, 1, \ldots, \tilde{N}+1)$.

Case I $\{m = \pi_{k+1}$ && $k \geq \tilde{N}\}$: In such a case, $\overline{\Phi}(m)s(k+1) = 0$ holds on the premise of $m = \pi_{k+1}$. Then, it can be derived that

$$\|\mathcal{P}_{\hbar+1}(\Phi(m))\| \leq c\sum_{q=0}^{\tilde{N}}a^q b w_0 + d w_0 + v_0 + \sum_{p=0}^{\tilde{N}}\frac{c^2 a^{\tilde{N}+q+1}}{\kappa\varepsilon}(c\sum_{q=0}^{\tilde{N}}a^q b w_0 + d w_0 + v_0)$$
$$= \varpi_{\tilde{N}+1} + \sum_{p=0}^{\tilde{N}}\frac{c^2 a^{\tilde{N}+p+1}}{\kappa\varepsilon}\varpi_p$$
$$= \frac{1}{2}\vec{\zeta}. \tag{27}$$

Case II $\{m = \pi_{k+1}$ && $k < \tilde{N}\}$: In this case, we have

$$\left\|\overline{\Phi}(m)\vec{o}(p)\right\| \leq c a^{k+1}\epsilon_0 + \varpi_{k+1} \leq \frac{1}{2}\overline{\zeta}. \tag{28}$$

Case III $\{m \neq \pi_{k+1}$ & & $k \geq \tilde{N}\}$: Note that $\overline{\Phi}(m)s(k+1) = \Phi(\pi_{k+1})\zeta(k+1) \neq 0$. Therefore, by using the method of scaling, it can be obtained that

$$\begin{aligned}\|\mathscr{P}_{k+1}(\Phi(m))\| \geq & \|\Phi(\pi_{k+1})\zeta(k+1)\| - c\sum_{q=0}^{\tilde{N}} a^q b w_0 - d w_0 - v_0 \\ & + \sum_{p=0}^{\tilde{N}} \frac{c^2 a^{\tilde{N}+q+1}}{\kappa\varepsilon}(c\sum_{q=0}^{\tilde{N}} a^q b w_0 + d w_0 + v_0) \\ & > \max\{\vec{\zeta}, \overline{\zeta}\} - \frac{1}{2}\vec{\zeta} \geq \frac{1}{2}\vec{\zeta}. \end{aligned} \tag{29}$$

Case IV $\{m \neq \pi_{k+1}$ & & $k < \tilde{N}\}$: Similar to the cases presented above, it is effortless to get

$$\left\|\overline{\Phi}(m)\vec{o}(p)\right\| > \frac{1}{2}\overline{\zeta}. \tag{30}$$

At last, utilizing mathematical induction from the (27)–(30), acquiring $\pi_k = \hat{\pi}_k$ for all values of k is not a difficult task. Hence, this finishes the proof. ∎

In the next part, Theorem 3 outlines the construction of artificial noise $\zeta(k)$ and introduces indicators that can evaluate the confidentiality performance.

Characterize secret capacity $\mathcal{S}_k$ with the following formula:

$$\mathcal{S}_k = \begin{cases} \log_2(1+\tilde{\psi}_k) - \log_2(1+\hat{\psi}_k), & if \quad \tilde{\psi}_k > \hat{\psi}_k, \\ 0, & if \quad \tilde{\psi}_k \leq \hat{\psi}_{,k} \end{cases} \tag{31}$$

where $\tilde{\psi}_k$ and $\hat{\psi}_k$ denote the received signal-to-noise ratios at the filter and potential eavesdroppers, respectively. Their values can be presented as

$$\begin{cases} \tilde{\psi}_k = \frac{\|y(k)\|^2}{\|y(k)-\hat{y}(k)\|^2}, \\ \hat{\psi}_k = \frac{\|y(k)\|^2}{\|y(k)-\bar{y}(k)\|^2}. \end{cases} \tag{32}$$

Theorem 3. *Set the artificial noise as* $\zeta(k) = (\max\{\max\ \{\vec{\zeta}, \overline{\zeta}\}, \delta_k\} + \varsigma_k)1_t$, *where* $\varsigma_k = \frac{\|y_k\|}{\sqrt{2^{1-\tau}-1}}$. $\tau \in (0,1)$ *denotes the confidentiality threshold. Hence,* $\mathcal{S}_k > \tau$ *holds for all* k.

Proof. Taking the norms of $\tilde{\psi}_k$ and $\hat{\psi}_k$ into consideration and noting that $\pi_k = \tilde{\pi}_k$, one has

$$\begin{aligned}\hat{y}(k) =& S(I - \Phi(\tilde{\pi}_k))S^T\bar{y}(k) \\ =& y(k) - S\Phi(\tilde{\pi}_k)S^T y(k), \end{aligned} \tag{33}$$

from which one can find the following inequalities hold:

$$\tilde{\psi}_k \geq \frac{1}{\|S\Phi(\pi_k)S^T\|^2} \geq \frac{1}{\lambda_{\max}(S\Phi(\pi_k)S^T)} \geq 1 \tag{34}$$

and

$$\hat{\psi}_k < \frac{\|y(k)\|^2}{\varsigma_k^2} = 2^{1-\tau} - 1. \tag{35}$$

Therefore it poses no difficulty to obtain $\tilde{\psi}_k > \hat{\psi}_k$ and the following formula holds:

$$\mathcal{S}_k = \log_2(1+\tilde{\psi}_k) - \log_2(1+\hat{\psi}_k) > 1 - \log_2(2^{1-\tau}) = \tau. \tag{36}$$

This finishes the proof. ∎

After the design of decryption function and the artificial noise in the aforementioned theorems, sufficient conditions will be provided to meet the H_∞ estimation performance index with the AETM and the designed EDM in Theorem 4.

Theorem 4. *For the given parameters $\chi, \rho, \gamma > 0$, $\overline{\alpha}, \lambda, \sigma \in (0,1)$ and filter gains $K_{r,\tilde{\pi}_k}(k)$, the H_∞ estimation performance of the augmented fuzzy system is satisfied if there exist positive definite matrices $P_{m,k}$ meeting the following equalities*:

$$\lambda - \frac{1}{\chi} \geq 0, \tag{37}$$

$$\tilde{\Pi}_{r,g,m}(k) < 0, \tag{38}$$

where

$$\tilde{\Pi}_{r,g,m}(k) = \Pi_{r,g,t}(k) + \Sigma_{r,g}(k), \Sigma_{r,g}(k) = \begin{bmatrix} \Lambda_{r,g}(k) & * \\ 0 & 0 \end{bmatrix},$$

$$\Lambda_{r,g}(k) = \overline{M}_{g,r}^T \overline{M}_{g,r} + \begin{bmatrix} 0 & * & * \\ 0 & 0 & * \\ 0 & 0 & -\gamma^2 I \end{bmatrix}, \Pi_{r,g,m}(k) = \begin{bmatrix} \nabla_{11} & * & * & * & * \\ \nabla_{21} & \nabla_{22} & * & * & * \\ \nabla_{31} & \nabla_{32} & \nabla_{33} & * & * \\ \nabla_{41} & \nabla_{42} & \nabla_{43} & \nabla_{44} & * \\ 0 & 0 & 0 & 0 & \nabla_{55} \end{bmatrix},$$

$$\nabla_{11} = \bar{A}_{g,r,\tilde{\pi}_k}^T \overline{P}_{k+1} \bar{A}_{g,r,\tilde{\pi}_k} + \overline{\mathcal{G}}(k) + \overline{\chi}\tilde{\mathcal{C}}(k) - P_{m,k}, \nabla_{21} = \overline{\alpha}\overline{B}_{r,\tilde{\pi}_k}^T \overline{P}_{k+1} \bar{A}_{g,r,\tilde{\pi}_k},$$

$$\nabla_{22} = \overline{\alpha}\overline{B}_{r,\tilde{\pi}_k}^T \overline{P}_{k+1} \overline{B}_{r,\tilde{\pi}_k} - I, \nabla_{31} = \overline{D}_{g,r,\tilde{\pi}_k}^T \overline{P}_{k+1} \bar{A}_{g,r,\tilde{\pi}_k} + \tilde{\mathcal{D}}(k),$$

$$\nabla_{32} = \overline{\alpha}\overline{D}_{g,r,\tilde{\pi}_k}^T \overline{P}_{k+1} \overline{B}_{r,\tilde{\pi}_k}, \nabla_{33} = \overline{D}_{g,r,\tilde{\pi}_k}^T \overline{P}_{k+1} \overline{D}_{g,r,\tilde{\pi}_k} + \overline{\chi} D^T(k) D(k),$$

$$\nabla_{41} = \bar{E}_{r,\tilde{\pi}_k}^T \overline{P}_{k+1} \bar{A}_{g,r,\tilde{\pi}_k}, \nabla_{42} = \overline{\alpha}\bar{E}_{r,\tilde{\pi}_k}^T \overline{P}_{k+1} \overline{B}_{r,\tilde{\pi}_k}, \nabla_{43} = \bar{E}_{r,\tilde{\pi}_k}^T \overline{P}_{k+1} \overline{D}_{g,r,\tilde{\pi}_k},$$

$$\nabla_{44} = \bar{E}_{r,\tilde{\pi}_k}^T \overline{P}_{k+1} \bar{E}_{r,\tilde{\pi}_k} - (\frac{1}{\chi} + \rho) I, \nabla_{55} = \frac{1}{\chi}(\lambda + \rho - 1) I, \overline{\chi} = \sigma(\frac{1}{\chi} + \rho),$$

$$P_{m,k} = diag\{P_{1,m,k}, P_{2,m,k}, P_{3,m,k}\}, \overline{P}_{k+1} = diag\{\overline{P}_{1,k+1}, \overline{P}_{2,k+1}, \overline{P}_{3,k+1}\},$$

$$\overline{P}_{j,k+1} = \sum_{q=1}^{t} p_q P_{j,q,k+1}, (j = 1,2,3), \tilde{\mathcal{D}}(k) = \begin{bmatrix} \overline{\chi} D^T(k) D(k) & 0 & 0 \end{bmatrix},$$

$$\overline{\mathcal{G}}(k) = \begin{bmatrix} \mathcal{G}^T\mathcal{G} & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{bmatrix}, \tilde{\mathcal{C}}(k) = \begin{bmatrix} C^T(k) C(k) & * & * \\ 0 & 0 & * \\ 0 & 0 & 0 \end{bmatrix}.$$

Proof. According to (3) and (5), it is easily derived that

$$\sigma y^T(k) y(k) - \Delta^T(k)\Delta(k) + \frac{1}{\chi}\epsilon(k) \geq 0, (k \in [t_n, t_{n+1})). \tag{39}$$

In light of (4) and (39), by using the iterative algorithm, one has

$$\begin{aligned}\epsilon(k+1) =&\sigma y^T(k)y(k) - \Delta^T(k)\Delta(k) + \lambda\epsilon(k)\\ \geq&\lambda\epsilon(k) - \frac{1}{\chi}\epsilon(k) \geq \ \cdots \ \geq (\lambda - \frac{1}{\chi})^{k+1}\epsilon(0) \geq 0.\end{aligned} \tag{40}$$

Considering the AETM and the EDM, choose the following Lyapunov function

$$V(k) = \xi^T(k)P_{m,k}\xi(k) + \frac{1}{\chi}\epsilon(k), \tag{41}$$

where $m = \tilde{\pi}_k$.

Setting the difference as $\Delta V(k) = V(k+1) - V(k)$ and taking (4) and (11) into consideration, one has

$$\begin{aligned}E\{\Delta V(k)\} =&E\{\xi^T(k+1)P_{\tilde{m},k+1}\xi(k+1) + \frac{1}{\chi}\epsilon(k+1) - \xi^T(k)P_{m,k}\xi(k) - \frac{1}{\chi}\epsilon(k)\}\\ \leq&E\{\xi^T(k+1)P_{\tilde{m},k+1}\xi(k+1) - \xi^T(k)P_{m,k}\xi(k) + \frac{1}{\chi}\epsilon(k+1) - \frac{1}{\chi}\epsilon(k)\}\\ &+ x^T(k)\mathcal{G}_{\mathcal{J}}^T\mathcal{G}_{\mathcal{J}}x(k) - v^T(k)v(k) + \rho(\sigma y^T(k)y(k) - \Delta^T(k)\Delta(k) + \frac{1}{\chi}\epsilon(k)),\end{aligned} \tag{42}$$

where $\tilde{m} = \tilde{\pi}_{k+1}$.

Set $\eta(k) = \begin{bmatrix}\xi^T(k) & v^T(k) & w^T(k) & \Delta^T(k) & \sqrt{\epsilon(k)}^T\end{bmatrix}^T$ and substitute (17) into (41), then it is obvious that

$$\begin{aligned}E\{\Delta V(k)\} \leq&E\{\sum_{g=1}^{h}\sum_{r=1}^{h}\theta_g(x(k))\theta_r(\hat{x}(k))[\bar{A}_{g,r,\tilde{\pi}_k}\xi(k) + (\alpha(k)-\overline{\alpha})\overline{B}_{r,\tilde{\pi}_k}v(k) + \overline{\alpha}\overline{B}_{r,\tilde{\pi}_k}v(k)\\ &+ \overline{D}_{g,r,\tilde{\pi}_k}w(k) + \bar{E}_{r,\tilde{\pi}_k}\Delta(k)]^T\overline{P}_{k+1}[\bar{A}_{g,r,\tilde{\pi}_k}\xi(k) + (\alpha(k)-\overline{\alpha})\overline{B}_{r,\tilde{\pi}_k}v(k)\\ &+ \overline{\alpha}\overline{B}_{r,\tilde{\pi}_k}v(k) + \overline{D}_{g,r,\tilde{\pi}_k}w(k) + \bar{E}_{r,\tilde{\pi}_k}\Delta(k)] - \xi^T(k)P_{m,k}\xi(k)\\ &+ \frac{1}{\chi}[(\lambda-1)x(k) - \Delta^T(k)\Delta(k) + \sigma y^T(k)y(k)]\} + x^T(k)\mathcal{G}_{\mathcal{J}}^T\mathcal{G}_{\mathcal{J}}x(k) - v^T(k)v(k)\\ &+ \rho(\sigma y^T(k)y(k) - \Delta^T(k)\Delta(k) + \frac{1}{\chi}\epsilon(k))\\ =&\sum_{g=1}^{h}\sum_{r=1}^{h}\theta_g(x(k))\theta_r(\hat{x}(k))\eta^T(k)\Pi_{r,g,m}(k)\eta(k).\end{aligned} \tag{43}$$

On the basis of (18) and (43), it poses no difficulty for us to obtain

$$\begin{aligned}&E\{\Delta V(k)\} + E\{\tilde{z}^T(k)\tilde{z}(k)\} - \gamma^2\omega^T(k)\omega(k)\\ \leq&\sum_{g=1}^{h}\sum_{r=1}^{h}\theta_g(x(k))\theta_r(\hat{x}(k))\eta^T(k)\tilde{\Pi}_{r,g,m}(k)\eta(k).\end{aligned} \tag{44}$$

Noticing (37) and (38) in Theorem 4, it yields that

$$E\{\Delta V(k)\} + E\{\tilde{z}^T(k)\tilde{z}(k)\} - \gamma^2\omega^T(k)\omega(k) \leq 0. \tag{45}$$

Therefore, with the zero initialization $z(0) = 0$, integrating both sides of the inequality to time k from 0 to ∞ for (45), it is derived that

$$E\left\{\sum_{k=0}^{\infty}\left\|\tilde{z}(k)^2\right\|\right\} - \gamma^2\sum_{k=0}^{\infty}\|\omega(k)\|^2 \le 0 \tag{46}$$

which indicates the ideal H_∞ performance index is met. ∎

According to the sufficient conditions derived in Theorem 4, the time-varying fuzzy filter gains are devised in Theorem 5.

Theorem 5. *For predesigned parameters $\chi, \rho, \gamma > 0, \overline{\alpha}, \lambda, \sigma \in (0,1)$, the H_∞ performance of system (17) under the AETM and the EDM can be ensured if there exist positive definite matrices $P_{m,k}$ and matrices $\Omega_{r,\hat{m}}(k)$ satisfying the following inequalities*:

$$\tilde{\nabla}_{r,g,m}(k) = \begin{bmatrix} \tilde{\nabla}_{11} & * & * & * & * & * & * \\ 0 & \tilde{\nabla}_{22} & * & * & * & * & * \\ \tilde{\nabla}_{31} & 0 & \tilde{\nabla}_{33} & * & * & * & * \\ 0 & 0 & 0 & \tilde{\nabla}_{44} & * & * & * \\ 0 & 0 & 0 & 0 & \tilde{\nabla}_{55} & * & * \\ \tilde{\nabla}_{61} & \tilde{\nabla}_{62} & \tilde{\nabla}_{63} & \tilde{\nabla}_{64} & 0 & \tilde{\nabla}_{66} & * \\ 0 & \tilde{\nabla}_{72} & 0 & 0 & 0 & 0 & \tilde{\nabla}_{77} \end{bmatrix} < 0, \tag{47}$$

where

$$\tilde{\nabla}_{11} = \overline{\mathcal{G}}(k) + \overline{\chi}\tilde{\mathcal{C}}(k) + \overline{M}_{g,r}^T\overline{M}_{g,r} - P_{m,k}, \tilde{\nabla}_{22} = -I, \tilde{\nabla}_{31} = \tilde{\mathcal{D}}(k), \tilde{\nabla}_{33} = \overline{\chi}D^T(k)D(k) - \gamma^2 I,$$
$$\tilde{\nabla}_{44} = -(\frac{1}{\chi} + \rho)I, \tilde{\nabla}_{55} = \frac{1}{\chi}(\lambda + \rho - 1)I, \tilde{\nabla}_{61} = \tilde{A}_{g,r,\tilde{\pi}_k}, \tilde{\nabla}_{62} = \overline{\alpha}\tilde{B}_{r,\tilde{\pi}_k}, \tilde{\nabla}_{63} = \tilde{D}_{g,r,\tilde{\pi}_k},$$
$$\tilde{\nabla}_{64} = \tilde{E}_{r,\tilde{\pi}_k}, \tilde{\nabla}_{66} = \tilde{\nabla}_{77} = -\overline{P}_{k+1}, \tilde{\nabla}_{72} = \sqrt{\overline{\alpha} - \overline{\alpha}^2}\tilde{B}_{r,\tilde{\pi}_k}, \overline{\Omega}_{r,\tilde{\pi}_k}(k) = \overline{P}_{2,k+1}K_{r,\tilde{\pi}_k}(k),$$
$$\tilde{A}_{g,r,\tilde{\pi}_k} = \begin{bmatrix} \tilde{a}_{11} & 0 & 0 \\ \tilde{a}_{21} & \tilde{a}_{22} & \tilde{a}_{23} \\ \tilde{a}_{31} & 0 & \tilde{a}_{33} \end{bmatrix}, \tilde{B}_{r,\tilde{\pi}_k}^T = \begin{bmatrix} 0 & \tilde{b}_{21} & \tilde{b}_{31} \end{bmatrix}^T, \tilde{D}_{g,r,\tilde{\pi}_k}^T = \begin{bmatrix} \tilde{\vartheta}_{11} & \tilde{\vartheta}_{21} & \tilde{\vartheta}_{31} \end{bmatrix}^T, \tilde{E}_{r,\tilde{\pi}_k}^T = \begin{bmatrix} 0 & \tilde{e}_{21} & \tilde{e}_{31} \end{bmatrix}^T,$$
$$\tilde{a}_{11} = \overline{P}_{1,k+1}A_g(k), \tilde{a}_{21} = \overline{P}_{1,k+1}A_g(k) - \overline{P}_{1,k+1}A_r(k) - (\beta_k - 1)\overline{\Omega}_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)C(k),$$
$$\tilde{a}_{22} = \overline{P}_{2,k+1}A_r(k) - \overline{\Omega}_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)C(k), \tilde{a}_{23} = (\beta_k - 1)\overline{\Omega}_{r,\tilde{\pi}_k}(k), \tilde{a}_{31} = \beta_k\overline{P}_{3,k+1}\tilde{\Phi}(\tilde{\pi}_k)C(k),$$
$$\tilde{b}_{21} = -\beta_k\overline{\Omega}_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k), \tilde{b}_{31} = \beta_k\overline{P}_{3,k+1}\tilde{\Phi}(\tilde{\pi}_k), \tilde{\vartheta}_{21} = \overline{P}_{2,k+1}B_g(k) - \beta_k\overline{\Omega}_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k)D(k),$$
$$\tilde{\vartheta}_{31} = \beta_k\overline{P}_{3,k+1}\tilde{\Phi}(\tilde{\pi}_k)D(k), \tilde{e}_{21} = \beta_k\overline{\Omega}_{r,\tilde{\pi}_k}(k)\tilde{\Phi}(\tilde{\pi}_k), \tilde{e}_{31} = -\beta_k\overline{P}_{3,k+1}\tilde{\Phi}(\tilde{\pi}_k).$$

Proof. Define

$$\overline{\Omega}_{r,\tilde{\pi}_k}(k) = K_{r,\tilde{\pi}_k}(k)\overline{P}_{j,k+1}. \tag{48}$$

On the basis of sufficient condition in (38), by using the Schur Complement Lemma, the matrices inequalities(47) can be derived from (38). Additionally, the time-varying fuzzy filter gains are calculated as $K_{r,\tilde{\pi}_k}(k) = \overline{P}_{1,k+1}^{-1}\overline{\Omega}_{r,\tilde{\pi}_k}(k)$. The proof is now completed. ∎

TABLE 1 Membership functions with lower and upper bounds.

Lower bounds	Upper bounds
$\underline{Z}_1^1(x_1(k)) = 1 - e^{-\frac{x_1^2(k)}{1.35}}$	$\overline{Z}_1^1(x_1(k)) = 0.3e^{-\frac{x_1^2(k)}{0.25}}$
$\underline{Z}_2^1(x_1(k)) = 1 - 0.3e^{-\frac{x_1^2(k)}{0.25}}$	$\overline{Z}_2^1(x_1(k)) = e^{-\frac{x_1^2(k)}{1.35}}$
$\underline{Z}_1^2(x_1(k)) = 0.35e^{-\frac{x_1^2(k)}{0.23}}$	$\overline{Z}_1^2(x_1(k)) = e^{-\frac{x_1^2(k)}{2.6}}$
$\underline{Z}_2^2(x_1(k)) = 1 - e^{-\frac{x_1^2(k)}{2.6}}$	$\overline{Z}_2^2(x_1(k)) = 1 - 0.35e^{-\frac{x_1^2(k)}{0.23}}$

TABLE 2 Nonlinear weighting functions.

Lower bound weight	Upper bound weight
$\underline{o}_g(x(k)) = \sin^2(x_1(k))$	$\bar{o}_g(x(k)) = 1 - \sin^2(x_1(k))$

Remark 6. In contrast to other state estimation strategies in References 18 and 53, the use of the EDM may increase computational complexity to some extent, since it requires time to calculate the value of the decrypt function for different values of t and identify the value of t that minimizes the function. However, once the decryption function is determined, the evaluation is not overly complex. Furthermore, different from previous researches about the encryption-decryption-based recursive filter[43] and edge-event-triggered encryption-decryption observer-based controller,[44] this paper not only extends to the situation of privacy-preserving-based fuzzy filter under the impact of FDI attacks but also adopts a useful method to more effectively address the threat of key theft and ensure data security with minimal impact on filtering performance.

4 | NUMERICAL ILLUSTRATIVE EXAMPLE

A numerical illustrative example is conducted to validate the accuracy of the given EDM and assess the fuzzy filter estimation performance.

Consider system (1) with two rules, and the parameters are given by

$$A_1(k) = \begin{bmatrix} a_1 & 0.5 & 0.3 \\ 0.55 & a_2 & 0.59 \\ a_3 & 0.55 & -0.7 \end{bmatrix}, A_2(k) = \begin{bmatrix} 0.4 & a_4 & 0.2 \\ 0.41 & a_5 & 0.59 \\ -0.7 & a_6 & -0.49 \end{bmatrix}, C(k) = \begin{bmatrix} c_1 & -0.08 & -0.14 \\ -0.08 & 0.06 & -0.02 \\ 0.11 & 0.12 & c_2 \end{bmatrix},$$
$$B_1(k) = \begin{bmatrix} 0.09 & -0.15 & b_1 \end{bmatrix}^T, B_2(k) = \begin{bmatrix} 0.1 & 0.2 & b_2 \end{bmatrix}^T, D(k) = \begin{bmatrix} 0.08 & d_1 & 0.15 \end{bmatrix}^T,$$
$$M_1(k) = 0.5diag\{0.1, m_1, 0.2\}, M_2(k) = 0.3diag\{0.2, 0.1, m_2\},$$

where

$$a_1 = 0.5 + 0.01\cos(0.2(k-1)), a_2 = 0.43 - 0.01\sin(0.2(k-1)),$$
$$a_3 = -0.55 + 0.02\cos(0.2(k-1)), a_4 = 0.59 + 0.02\sin(0.2(k-1)),$$
$$a_5 = 0.5 - 0.02\sin(0.1(k-1)), a_6 = 0.6 - 0.01\cos(0.2(k-1)),$$
$$b_1 = 0.1 + 0.05\cos(0.1k), b_2 = 0.05 + 0.02\sin(0.1k),$$
$$c_1 = -0.06 + 0.01\cos(0.2(k-1)), c_2 = 0.19 - 0.01\sin(0.3(k-1)),$$
$$d_1 = 0.1 + 0.02\cos(k-1), m_1 = 0.015 - 0.1\sin(k-1), m_2 = 0.1 + 0.1\cos(k-1).$$

Hence, it is not hard to acquire the upper bounds for the norm of the plant parameters satisfy $a = 1.24, b = 0.19, c = 0.28, d = 0.21$.

The membership functions and the nonlinear weighting functions are listed in Table 1 and Table 2, respectively.

In this example, the initial condition of state values is depicted as $x(0) = \begin{bmatrix} 0.5 & 0.7 & 0.6 \end{bmatrix}^T$, $\hat{x}(0) = \begin{bmatrix} 0.3 & 0.4 & 0.5 \end{bmatrix}^T$. Set the disturbance input as $w(k) = 0.01sin(0.3k)$ and performance index $\gamma = 0.8$.

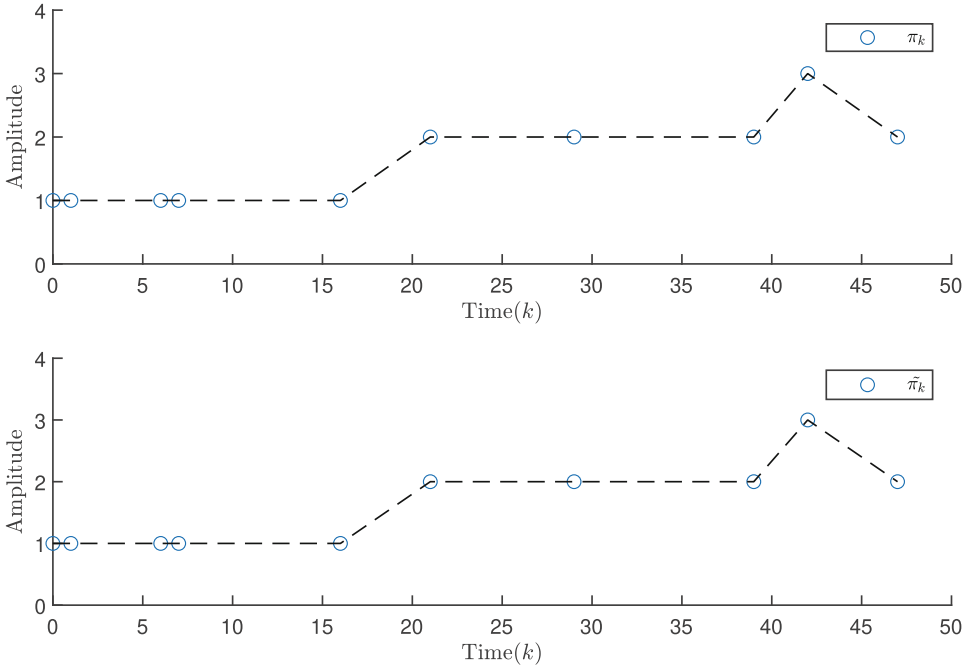

FIGURE 1 The values of π_k and $\tilde{\pi}_k$ at triggering instants.

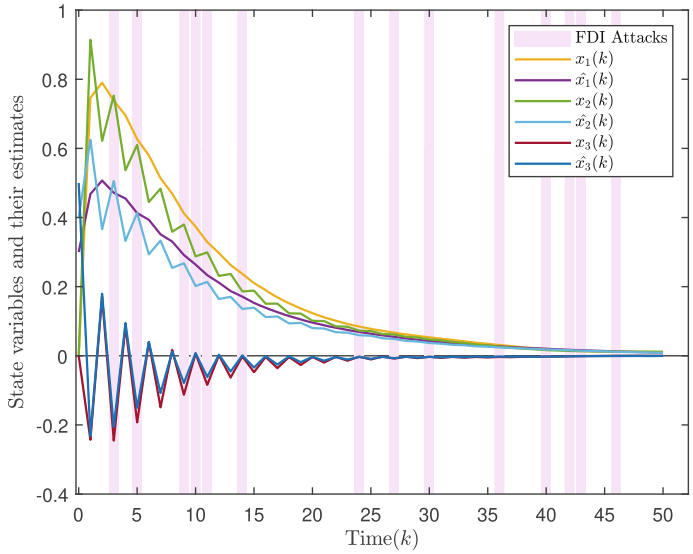

FIGURE 2 State trajectories and their estimates.

The AETM parameters are given as $\chi = 5$, $\lambda = 0.7$, $\sigma = 0.5$ and the initial dynamic threshold $\epsilon_0 = 1$. What's more, the probability of the FDI attacks is $\overline{\alpha} = 0.3$ and the FDI attack signals are described as $v(k) = diag\{0.1sin(k-1), 0.1sin(k-1), 0.1sin(k-1)\}x(k)$ with the matrix $\mathcal{G} = diag\{0.1, 0.1, 0.1\}$.

As to the EDM, the occurrence possibilities are $p_1 = 0.35, p_2 = 0.32, p_3 = 0.33$. Set the secret key as the following orthogonal matrix:

$$S = \begin{bmatrix} -0.6 & -0.8 & 0 \\ -0.8 & 0.6 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

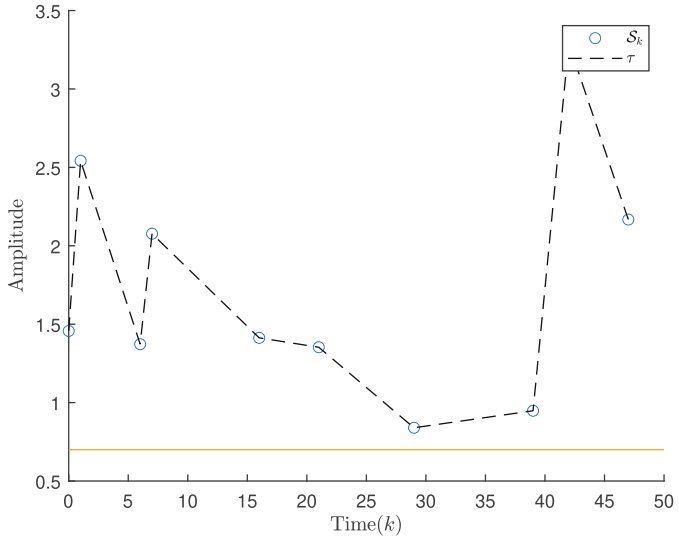

FIGURE 3 The values of $\mathcal{S}_k$ and τ at triggering instants.

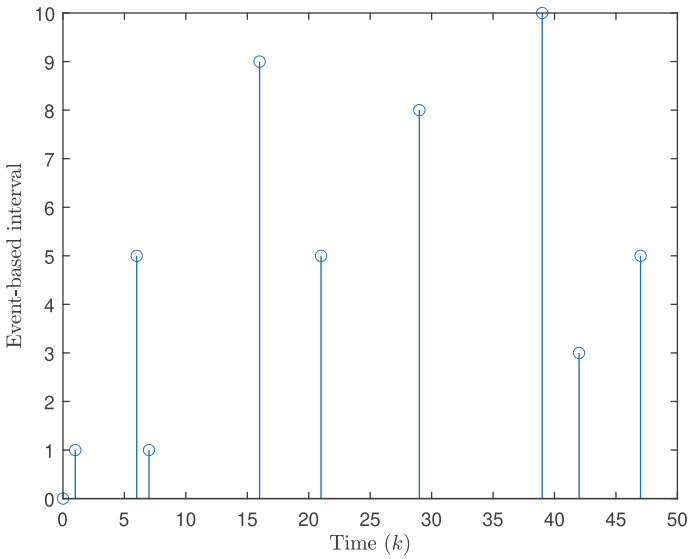

FIGURE 4 The release instants of AETM.

To meet the conditions proposed by Definition 1, Assumptions 1 and 2, set the parameters as $\varepsilon = 0.01, \kappa = 0.2, \tilde{N} = 6, \epsilon_0 = 1.1, w_0 = 0.01, v_0 = 0.12$. The other parameters are given to be $\tau = 0.7, \rho = 0.001$.

The trajectories of the randomly selected nodes due to probability distribution at triggering moments and its estimated value are shown in Figure 1. It is straightforward that the estimated value $\tilde{\pi}_k$ matches the value of π_k chosen through a probabilistic selection process.

Remark 7. Since the chosen nodes solved at the decrpytion process are consistent with the randomly selected nodes during the encryption process, one can validate the correctness of suggested EDM. Compared with the normal secret-key-based EDM, the EDM employed in this paper, on the premise of ensuring the accuracy of the encryption and decryption process, has higher randomness owing to nodes randomly selected according to probability distribution. This greatly enhances the data security against eavesdropping attacks under key theft.

In Figure 2, it shows the trajectories of state values and their corresponding estimated values, from which one can obviously witness the estimated value of the fuzzy filter $\hat{x}(k)$ can effectively follow $x(k)$ under the impact of FDI attacks.

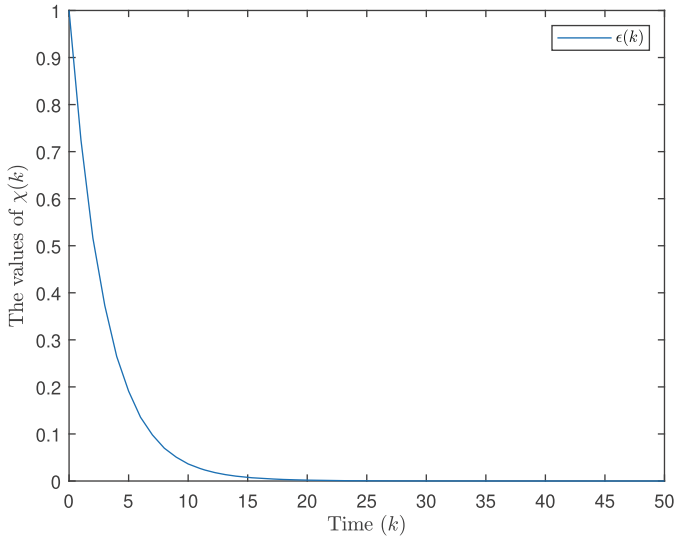

FIGURE 5 The values of dynamic threshold $\epsilon(k)$.

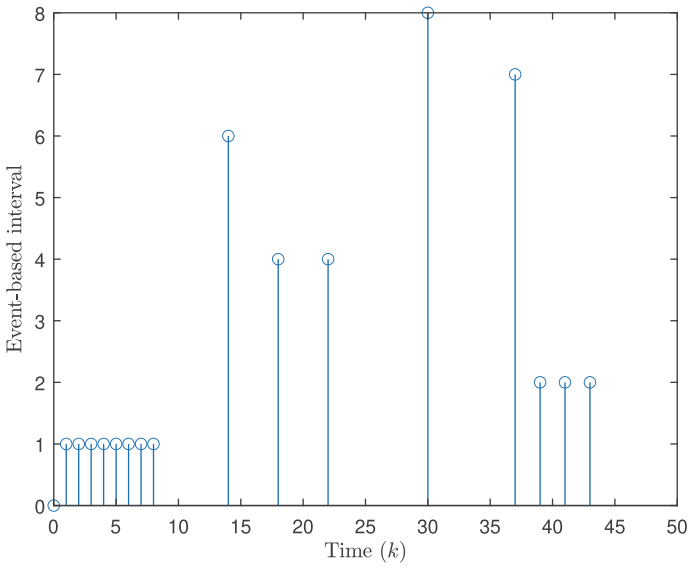

FIGURE 6 The release instants of SETM.

In Figure 3, it reveals the relationship between secret capacity $\mathcal{S}_k$ and the threshold τ. It is apparent that the value of $\mathcal{S}_k$ exceeds τ at all-time instants. Therefore, compared with traditional EDM, although our method may increase the computational complexity to a certain extent, it can still ensure that the estimation performance and confidentiality performance of the system meet expectations.

Under the AETM, the event trigger instants and the values of dynamic threshold $\chi(k)$ are depicted in Figure 4 and Figure 5, respectively. It is evident that the excessive data, excluding those meeting condition (3), are not sent through the communication channel. Specially, when $\theta \to \infty$, AETM will transition into a SETM. In comparison with the SETM, whose release instants are shown in Figure 6, more valuable information is transmitted under the AETM according to Table 3. It can be derived that only 20% of the sampling data can be transmitted under AETM, while the transmission rate under SETM is 34%. In conclusion, the proposed AETM can effectively lighten the communication burden compared with the SETM.

TABLE 3 Comparison between two event trigger mechanisms.

	AETM	SETM
Transmission instants	10	17
Transmission rate	20%	34%

5 | CONCLUSION

This article focuses on the privacy-preserving-based filtering issue for time-varying NSs at the risk of FDI attacks and potential information leakage. Taking the current situation into account, an AETM is employed to prevent data congestion in the network and ease the pressure on network communication. To accomplish the objective of privacy protection, the signal is encrypted by the inclusion of artificial noise, secret key, and the utilization of randomly selected nodes. According to the encryption scheme, the design of decryption function is strictly due to the encryption function and the transmitted signal. The filter is designed considering the EDM and then a fuzzy augmented error system is presented. Furthermore, sufficient conditions are provided for the augmented dynamics to achieve the desired disturbance attenuation level by selecting the proper Lyapunov functional candidate and the filter gains are obtained by resorting to recursive matrix inequalities. Finally, a simulation example is presented to validate both the correctness and effectiveness of the advocated algorithm. In future work, our attention will be paid to the combination of the communication protocol and EDM in the field of state estimation, along with the occurrence of hybrid cyber attacks.

FUNDING INFORMATION

This work was supported in part by the National Natural Science Foundation of China under Grant 62373252, and Grant 62273174, and in part by the Startup Foundation for Introducing Talent of NUIST under Grant 2024r063.

CONFLICT OF INTEREST STATEMENT

The authors declare no conflicts of interest.

DATA AVAILABILITY STATEMENT

Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

ORCID

Jinliang Liu https://orcid.org/0000-0001-5489-0246
Lijuan Zha https://orcid.org/0000-0003-0475-8866
Xiangpeng Xie https://orcid.org/0000-0003-4822-3134
Engang Tian https://orcid.org/0000-0002-8169-5347

REFERENCES

1. Liu SC, Lin SF. LMI-based robust sliding control for mismatched uncertain nonlinear systems using fuzzy models. *Int J Robust Nonlinear Control*. 2012;22(16):1827-1836.
2. Wang T, Gao H, Qiu J. A combined adaptive neural network and nonlinear model predictive control for multirate networked industrial process control. *IEEE Trans Neural Networks Learn Syst*. 2016;27(2):416-425.
3. Zha L, Huang T, Liu J, Xie X, Tian E. Outlier-resistant quantized control for T-S fuzzy systems under multi-channel-enabled round-robin protocol and deception attacks. *Int J Robust Nonlinear Control*. 2023;33(18):10916-10931.
4. Choi HD, Ahn CK, Shi P, Wu L, Lim MT. Dynamic output-feedback dissipative control for T–S fuzzy systems with time-varying input delay and output constraints. *IEEE Trans Fuzzy Syst*. 2017;25(3):511-526.
5. Shen H, Li F, Yan H, Karimi HR, Lam HK. Finite-time event-triggered H_∞ control for T–S fuzzy markov jump systems. *IEEE Trans Fuzzy Syst*. 2018;26(5):3122-3135.
6. Xie X, Yue D, Zhang H, Xue Y. Control synthesis of discrete-time T–S fuzzy systems via a multi-Instant homogenous polynomial approach. *IEEE Trans Cybern*. 2016;46(3):630-640.
7. Fan C, Lam J, Xie X. Fault estimation for periodic piecewise T-S fuzzy systems. *Int J Robust Nonlinear Control*. 2021;31(16):8055-8074.
8. Chen H, Zong G, Zhao X, Gao F, Shi K. Secure filter design of fuzzy switched CPSs with mismatched modes and application: A multidomain event-triggered strategy. *IEEE Trans Industr Inform*. 2023;19(10):10034-10044.

9. Yan JJ, Yang GH, Li XJ. Adaptive fault-tolerant compensation control for T–S fuzzy systems with mismatched parameter uncertainties. *IEEE Trans Syst Man Cybern Syst*. 2020;50(9):3412-3423.
10. Yu Z, Xu Y, Zhang Y, Jiang B, Su CY. Fractional-order fault-tolerant containment control of multiple fixed-wing UAVs via disturbance observer and interval type-2 fuzzy neural network. *Int J Robust Nonlinear Control*. 2023;33(17):10257-10277.
11. Yang Y, Niu Y, Lam J. Security interval type-2 fuzzy sliding mode control under multistrategy injection attack: design, analysis, and optimization. *IEEE Trans Fuzzy Syst*. 2023;31(9):2943-2955.
12. Yan C, Xia J, Park JH, Xie X. Reinforcement learning-based adaptive event-triggered fuzzy control for cyclic switched stochastic nonlinear systems with actuator faults. *IEEE Trans Fuzzy Syst*. 2023;32(3):1131-1143.
13. Liu J, Gong E, Zha L, Tian E, Xie X. Observer-based security fuzzy control for nonlinear networked systems under weighted try-once-discard protocol. *IEEE Trans Fuzzy Syst*. 2023;31(11):3853-3865.
14. Liu J, Yang M, Xie X, Peng C, Yan H. Finite-time H_∞ filtering for state-dependent uncertain systems with event-triggered mechanism and multiple attacks. *IEEE Trans Circuits Syst I Regular Pap*. 2020;67(3):1021-1034.
15. Li C, Wang Z, Song W, Zhao S, Wang J, Shan J. Resilient unscented Kalman filtering fusion with dynamic event-triggered scheme: Applications to multiple unmanned aerial vehicles. *IEEE Trans Control Syst Technol*. 2023;31(1):370-381.
16. Liu H, Wang Z, Fei W, Li J. Resilient H_∞ state estimation for discrete-time stochastic delayed memristive neural networks: A dynamic event-triggered mechanism. *IEEE Trans Cybern*. 2022;52(5):3333-3341.
17. Chen Y, Wang Z, Yuan Y, Date P. Distributed H_∞ filtering for switched stochastic delayed systems over sensor networks with fading measurements. *IEEE Trans Cybern*. 2020;50(1):2-14.
18. Ge X, Han QL, Zhang XM, Ding L, Yang F. Distributed event-triggered estimation over sensor networks: A survey. *IEEE Trans Cybern*. 2020;50(3):1306-1320.
19. Chen W, Wang Z, Hu J, Dong H, Liu GP. Distributed resilient state estimation for cyber-physical systems against bit errors: A zonotopic set-membership approach. *IEEE Trans Netw Sci Eng*. 2023;10(6):3922-3932.
20. Ding D, Wang Z, Han QL, Zhang XM. Recursive secure filtering over Gilbert-Elliott channels in sensor networks: the distributed case. *IEEE Trans Signal Informat Process Networks*. 2021;7:75-86.
21. Liu J, Gong E, Zha L, Tian E, Xie X. Interval type-2 fuzzy-model-based filtering for nonlinear systems with event-triggering weighted try-once-discard protocol and cyber-attacks. *IEEE Trans Fuzzy Syst*. 2023;32(3):721-732.
22. Yue D, Tian E, Han QL. A delay system method for designing event-triggered controllers of networked control systems. *IEEE Trans Autom Control*. 2013;58(2):475-481.
23. Liu J, Gu Y, Zha L, Liu Y, Cao J. Event-triggered H_∞ load frequency control for multiarea power systems under hybrid cyber attacks. *IEEE Trans Syst Man Cybern Syst*. 2019;49(8):1665-1678.
24. Ding L, Han QL, Ge X, Zhang XM. An overview of recent advances in event-triggered consensus of multiagent systems. *IEEE Trans Cybern*. 2018;48(4):1110-1123.
25. Gu Z, Shi P, Yue D, Yan S, Xie X. Fault estimation and fault-tolerant control for networked systems based on an adaptive memory-based event-triggered mechanism. *IEEE Trans Netw Sci Eng*. 2021;8(4):3233-3241.
26. Gu Z, Yan S, Ahn CK, Yue D, Xie X. Event-triggered dissipative tracking control of networked control systems with distributed communication delay. *IEEE Syst J*. 2022;16(2):3320-3330.
27. Gu Z, Shi P, Yue D, Yan S, Xie X. Memory-based continuous event-triggered control for networked T–S fuzzy systems against cyberattacks. *IEEE Trans Fuzzy Syst*. 2021;29(10):3118-3129.
28. Zhang L, Liang H, Sun Y, Ahn CK. Adaptive event-triggered fault detection scheme for semi-Markovian jump systems with output quantization. *IEEE Trans Syst Man Cybern Syst*. 2021;51(4):2370-2381.
29. Xu Y, Sun J, Wu ZG, Wang G. Fully distributed adaptive event-triggered control of networked systems with actuator bias faults. *IEEE Trans Cybern*. 2022;52(10):10773-10784.
30. Wang X, Ding D, Ge X, Han QL. Neural-network-based control for discrete-time nonlinear systems with denial-of-service attack: the adaptive event-triggered case. *Int J Robust Nonlinear Control*. 2022;32(5):2760-2779.
31. Ju Y, Ding D, He X, Han QL, Wei G. Consensus control of multi-agent systems using fault-estimation-in-the-loop: dynamic event-triggered case. *IEEE/CAA J Automat Sinica*. 2022;9(8):1440-1451.
32. Liu J, Zhang N, Zha L, Xie X, Tian E. Reinforcement learning-based decentralized control for networked interconnected systems with communication and control constraints. *IEEE Trans Autom Sci Eng*. 2023. doi:10.1109/TASE.2023.3300917
33. Zhang Y, Peng C, Cheng C, Wang YL. Attack intensity dependent adaptive load frequency control of interconnected power systems under malicious traffic attacks. *IEEE Trans Smart Grid*. 2023;14(2):1223-1235.
34. Wu J, Peng C, Zhang J, Tian E. A sampled-data-based secure control approach for networked control systems under random DoS attacks. *IEEE Trans Cybern*. 2024. doi:10.1109/TCYB.2024.3350331
35. Liu J, Dong Y, Zha L, Xie X, Tian E. Reinforcement learning-based tracking control for networked control systems with DoS attacks. *IEEE Trans Inf Forensics Secur*. 2024. doi:10.1109/TIFS.2024.3376250
36. Chen B, Tan Y, Sun Z, Yu L. Attack-resilient control against FDI attacks in cyber-physical systems. *IEEE/CAA J Automat Sinica*. 2022;9(6):1099-1102.
37. Qi W, Hou Y, Zong G, Ahn CK. Finite-time event-triggered control for semi-Markovian switching cyber-physical systems with FDI attacks and applications. *IEEE Trans Circuits Syst I Regular Pap*. 2021;68(6):2665-2674.
38. Li Y, Song F, Liu J, Xie X, Tian E. Software-defined event-triggering control for large-scale networked systems subject to stochastic cyberattacks. *IEEE Trans Control Netw Syst*. 2023;10(3):1531-1541.

39. Hu S, Ge X, Li Y, Chen X, Xie X, Yue D. Resilient load frequency control of multi-area power systems under DoS attacks. *IEEE Trans Inf Forensics Secur*. 2023;18:936-947.
40. Zhang Y, Wu ZG. Asynchronous control of Markov jump systems under aperiodic DoS attacks. *IEEE Trans Circuits Syst II Express Briefs*. 2023;70(2):685-689.
41. Guo H, Pang ZH, Sun J, Li J. An output-coding-based detection scheme against replay attacks in cyber-physical systems. *IEEE Trans Circuits Syst II Express Briefs*. 2021;68(10):3306-3310.
42. Xu X, Li X, Dong P, Liu Y, Zhang H. Robust reset speed synchronization control for an integrated motor-transmission powertrain system of a connected vehicle under a replay attack. *IEEE Trans Veh Technol*. 2021;70(6):5524-5536.
43. Zou L, Wang Z, Shen B, Dong H. Encryption-decryption-based state estimation with multi-rate measurements against eavesdroppers: A recursive minimum-variance approach. *IEEE Trans Autom Control*. 2023;68(12):8111-8118.
44. Guo XG, Wang BQ, Wang JL, Ahn CK, Wu ZG. Edge-event-triggered encryption-decryption observer-based control of multiagent systems for privacy protection under multiple cyber attacks. *Inf Sci*. 2023;642:119128.
45. Li T, Wang Z, Zou L, Chen B, Yu L. A dynamic encryption–decryption scheme for replay attack detection in cyber–physical systems. *Automatica*. 2023;151:110926.
46. Lu J, Leong AS, Quevedo DE. Optimal event-triggered transmission scheduling for privacy-preserving wireless state estimation. *Int J Robust Nonlinear Control*. 2020;30(11):4205-4224.
47. Zou L, Wang Z, Shen B, Dong H, Lu G. Encrypted finite-horizon energy-to-peak state estimation for time-varying systems under eavesdropping attacks: Tackling secrecy capacity. *IEEE/CAA J Automat Sinica*. 2023;10(4):985-996.
48. Yan J, Meng Y, Yang X, Luo X, Guan X. Privacy-preserving localization for underwater sensor networks via deep reinforcement learning. *IEEE Trans Inf Forensics Secur*. 2021;16:1880-1895.
49. Sun L, Ding D, Dong H, Bai X. Privacy-preserving distributed economic dispatch for microgrids based on state decomposition with added noises. *IEEE Trans Smart Grid*. 2024;15(3):2424-2433. doi:10.1109/TSG.2023.3324138
50. Zhang S, Ma L, Liu H. Encryption-decryption-based event-triggered consensus control for nonlinear MASs under DoS attacks. *Int J Robust Nonlinear Control*. 2024;34(1):132-146. doi:10.1002/rnc.6964
51. Pang ZH, Fan LZ, Dong Z, Han QL, Liu GP. False data injection attacks against partial sensor measurements of networked control systems. *IEEE Trans Circuits Syst II Express Briefs*. 2022;69(1):149-153.
52. Reif K, Gunther S, Yaz E, Unbehauen R. Stochastic stability of the discrete-time extended Kalman filter. *IEEE Trans Autom Control*. 1999;44(4):714-728.
53. Han M, Lam HK, Liu F, Tang Y, Zhou H. Estimation of domain of attraction for discrete-time positive interval type-2 polynomial fuzzy systems with input saturation. *IEEE Trans Fuzzy Syst*. 2022;30(2):397-411.

How to cite this article: Liu J, Tang J, Zha L, Xie X, Tian E, Peng C. Privacy-preserving-based fuzzy filtering for nonlinear networked systems with adaptive-event-triggered mechanism and FDI attacks. *Int J Robust Nonlinear Control*. 2024;34(14):9716-9736. doi: 10.1002/rnc.7489