IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received 12 March 2024, accepted 27 March 2024, date of publication 2 April 2024, date of current version 9 April 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3384237

RESEARCH ARTICLE

$\mathcal{H}_\infty$ Filtering for Discrete-Time Singular Markov Jump Systems Under DoS Attacks and Its Application

LING CHEN[1], GUANQI WANG[2], AND FENG LI[2]
[1]School of Electrical and Information Engineering, Wanjiang University of Technology, Ma'anshan 243031, China
[2]School of Electrical and Information Engineering, Anhui University of Technology, Ma'anshan 243002, China

Corresponding author: Feng Li (fengli4131@gmail.com)

This work was supported in part by the Key Natural Science Foundation of Higher Education Institutions of Anhui Province under Grant 2023AH052495, and in part by the Key Project of Natural Science Research in Universities of Anhui Province under Grant 2022AH050328.

ABSTRACT This study addresses $\mathcal{H}_\infty$ filtering against DoS attacks within the framework of singular Markov jump systems. To provide a more comprehensive depiction of the issue pertaining to cyber security, DoS attacks are perceived as occurring in an unpredictable manner and can be represented by a collection of a random variable that follows the Bernoulli distribution. Consequently, the corresponding filter error system is formulated. Utilizing a set of viable linear matrix inequalities, this research establishes criteria of stochastically admissible for filter error system, ensuring a specified $\mathcal{H}_\infty$ performance. A filter design method under DoS attacks is proposed. Finally, the effectiveness of this method is demonstrated through a practical example involving a tunnel diode model.

INDEX TERMS Bernoulli distribution, singular Markov jump system, denial of service (DoS) attacks, tunnel diode model.

I. INTRODUCTION

Stochastic phenomena are often exist in control systems, which may be caused by changes in certain correlated structures between subsystems. Markov jump systems are renowned for their ability to model dynamic systems with abrupt changes [1], [2]. Singular systems, as a special dynamic system model in a more general form than state-space systems, can better describe a class of complex systems with singular properties, and they have been widely used in electric power systems, circuit systems, and astronautical systems. Besides, random abrupt factors such as failure occurrence can lead to mutations in its own structure and parameters [3], [4], [5], [6]. When the parameters of the singular system are mutated, some researchers built singular Markov jump systems (SMJSs). SMJSs combine properties of both singular systems and Markov jump systems. As a type of stochastic hybrid system, SMJSs can be used for modeling the actual systems. Up to now, numerous research findings on SMJSs have sprung up, such as stability research on SMJSs [7], time-delay problem [8], and design results of controllers and observers [9], [10], [11].

In addition, security issues under network attacks have attracted much attention [12], [13], [14], [15], [16]. When it comes to cybersecurity, one must pay attention to the growing threat of cyber attacks. Network attacks refers to the use of computer network system vulnerabilities or weaknesses, malicious operation or interference behavior. These attacks can take a variety of forms, with one common form of attack being DoS attack. DoS attacks are a common, simple, effective, and extremely harmful method among many network attack techniques. Their main method of attack is to maliciously consume network bandwidth and system resources, causing system paralysis and disabling the function of serving normal users, thereby denying them access to services [17], [18], [19]. In network security, it is very important to prevent and deal with DoS attacks.

The associate editor coordinating the review of this manuscript and approving it for publication was Xiaojie Su.

TABLE 1. Notation clarification in this article.

Symbols	Clarification
$\mathbb{R}^{\kappa\times\kappa}$	$\kappa\times\kappa$ real matrix.
$Sym\{W\}$	$W+W^T$.
$\mathbb{E}$	Expected value
$*$	Symmetric matrix element.
$\Pr\{\cdot\}$	Probability value.

Moreover, the issue of filtering has consistently been a focal point of investigation in the field of control. The primary goal is to eliminate specific interference, interruptions, or frequency elements in the initial signal to ensure that the final signal accurately represents the properties of the input signal. Compared with kalman filtering, $\mathcal{H}_\infty$ filtering offers significant advantages in estimation accuracy and robustness.

However, based on the above analysis, the problem of filtering under DoS attack in SMJSs and its application have not been solved, which is the motivation of this paper. The main contributions include the following two aspects:

(I) This article presents the $\mathcal{H}_\infty$ filtering issue for SMJSs under the impact of DoS attacks. It is worth mentioning that the DoS attacks can be represented by a random variable that follows Bernoulli distribution. And the filter gains are computed, leading to the proposal of a method for secure filter design for SMJSs.

(II) For the first time, an efficient criterion is established for filter error systems (FES) within the context of SMJSs. Furthermore, this criterion is applicable to systems experiencing DoS attacks. Ultimately, the effectiveness of the suggested approach is confirmed through experimentation with a circuit containing a tunnel diode.

The notation used in this work is given in Table 1.

II. PROBLEM FORMULATION

Following is the SMJSs:

$$\begin{cases} Ex(\zeta+1) = A(\varphi_\zeta)x(\zeta) + B(\varphi_\zeta)w(\zeta) \\ y(\zeta) = C(\varphi_\zeta)x(\zeta) + D(\varphi_\zeta)w(\zeta) \\ z(\zeta) = Q(\varphi_\zeta)x(\zeta) \end{cases} \tag{1}$$

where $x(\zeta)\in\mathbb{R}^\kappa$ denotes the system state, $y(\zeta)\in\mathbb{R}^\delta$ represents the measured output, and $z(\zeta)\in\mathbb{R}^\tau$ signifies the estimated signal. Matrix $E\in\mathbb{R}^{\kappa\times\kappa}$ is singular with $rank(E)=\varrho\leq\kappa$. The sequence $\{\varphi_\zeta\}$ constitutes a Markov chain that takes value in a limited state space $Y=\{1,2,\cdots,y\}$. The transitions between states adhere to the rules dictated by the Markov chain, which characterized by the following transition probability:

$$\pi_{rd} = \Pr\{\varphi_{\zeta+1}=d \mid \varphi_\zeta = r\},$$

where $0\leqslant\pi_{rd}\leqslant 1$, $\sum_{d=1}^{y}\pi_{rd}=1$.

Remark 1: Singular systems poses greater challenges due to the potential occurrence of incompatible phenomena within their homogeneous initial value problems, setting them apart from state space systems. Additionally, the complexity arising from multi-mode jumps and nonlinear factors complicates system analysis, often leaving their control issues largely unexplored.

We can obtain that:

$$\begin{cases} Ex(\zeta+1) = A_r x(\zeta) + B_r w(\zeta) \\ y(\zeta) = C_r x(\zeta) + D_r w(\zeta) \\ z(\zeta) = Q_r x(\zeta) \end{cases} \tag{2}$$

The expression for the $\tilde{y}(\zeta)$ can be reformulated as follows:

$$\tilde{y}(\zeta) = \bar{\mu}(\zeta)y(\zeta). \tag{3}$$

The variable $\bar{\mu}(\zeta))$ is a random variable describing attack occurrences, which follows Bernoulli distribution. A value of 0 indicates a DoS attack occurs, while a value of 1 signifies the absence of an attack. The probability value is as follows:

$$\Pr\{\bar{\mu}(\zeta)=1\} = \bar{\mu}$$

The variable $\bar{\mu}$ resides within the range [0, 1] and signifies the probability of DoS attacks.

$$\mathbb{E}\{\bar{\mu}(\zeta)\} = \bar{\mu}, \quad \mathbb{E}\{\bar{\mu}(\zeta)-\bar{\mu}\} = 0$$
$$\mathbb{E}\left\{|\ \bar{\mu}(\zeta)-\bar{\mu}\ |^2\right\} = \bar{\mu}(1-\bar{\mu}).$$

Remark 2: Cyber security has emerged as a pervasive issue, with network systems encountering escalating risks due to the impact of network attacks. DoS attacks involve hackers employing diverse attack methods to disrupt services, potentially leading to system destruction and network incapacitation. Based on the above analysis, we consider the DoS attacks in this paper.

The filter under possible DoS attacks can be designed as

$$\begin{cases} \tilde{x}(\zeta+1) = A_{fr}\tilde{x}(\zeta) + B_{fr}\bar{\mu}(\zeta)\{C_r x(\zeta) + D_r w(\zeta)\} \\ \tilde{z}(\zeta) = C_{fr}\tilde{x}(\zeta) \end{cases} \tag{4}$$

where A_{fr}, B_{fr}, C_{fr} are the filter parameters.

The following FES can be obtained from (2) and (4), where $\psi(\zeta) = \left[x^T(\zeta)\ \tilde{x}^T(\zeta)\right]^T$, $e(\zeta) \triangleq z(\zeta)-\tilde{z}(\zeta)$.

$$\begin{cases} \hat{E}\psi(\zeta+1) = \mathbb{A}_r\psi(\zeta) + \mathbb{B}_r w(\zeta) + (\bar{\mu}(\zeta)-\bar{\mu}) \\ \{\mathbb{C}_r\psi(\zeta) + \mathbb{D}_r w(\zeta)\} \\ e(\zeta) = \Theta_r\psi(\zeta) \end{cases} \tag{5}$$

where

$$\hat{E} \triangleq \mathrm{diag}\{E, I\},\ \Theta_r = \begin{bmatrix} Q_r^T \\ -C_{fr}^T \end{bmatrix}^T,$$
$$\mathbb{A}_r = \begin{bmatrix} A_r & 0 \\ \bar{\mu}B_{fr}C_r & A_{fr} \end{bmatrix},\ \mathbb{B}_r = \begin{bmatrix} B_r \\ \bar{\mu}B_{fr}D_r \end{bmatrix}$$
$$\mathbb{C}_r = \begin{bmatrix} 0 & 0 \\ B_{fr}C_r & 0 \end{bmatrix},\ \mathbb{D}_r = \begin{bmatrix} 0 \\ B_{fr}D_r \end{bmatrix}.$$

Definition 1: [20] The system (5) is regular and causal, if the following conditions meet:

$$\det\left(s\hat{E}-\mathbb{A}_r\right)\neq 0$$
$$\deg\left(\det\left(s\hat{E}-\mathbb{A}_r\right)\right)=\operatorname{rank}\left(\hat{E}\right)$$

with $w(\zeta)\equiv 0$.

Definition 2: [21] The system (5) is considered stochastically admissible when $w(\zeta)\equiv 0$, given that FES satisfies both regularity and causality criteria:

$$\sum_{\zeta=0}^{\infty}\mathbb{E}\left\{\|\ \psi(\zeta)\ \|^2|\ \psi(0),\varphi(0)\right\}<\infty$$

Definition 3: [22] The system represented by (5) maintains an $\mathcal{H}_\infty$ performance index γ, when $e(\zeta)$ fulfills:

$$\mathbb{E}\left\{\sum_{\zeta=0}^{\infty}e^T(\zeta)e(\zeta)\right\}<\gamma^2\sum_{\zeta=0}^{\infty}w^T(\zeta)w(\zeta).$$

with zero-initial conditions.

III. MAIN RESULTS

Theorem 1: The FES (5) achieves stochastic admissibility and attains an $\mathcal{H}_\infty$ performance level $\gamma>0$, for given a contant $\bar{\mu}\in[0,1]$, and a matrix $\tilde{\Phi}=\left[\Phi^T\ 0\right]^T$ fullfills $\hat{E}^T\tilde{\Phi}=0$, alongside the existence of matrix $\widetilde{\Lambda}_r=\left[\widetilde{\Lambda}_{1r}\ \widetilde{\Lambda}_{2r}\right]^T$ and symmetric positive definite matrix $\bar{P}_r$, conforming to the following condition:

$$\Re_r=\begin{bmatrix}\mathbb{Q}_r & \mathbb{R}_r & \Theta_r^T & \mathbb{A}_r^T & \mathbb{H}_r\\ * & -\gamma^2 I & 0 & \mathbb{B}_r^T & \mathbb{Z}_r\\ * & * & -I & 0 & 0\\ * & * & * & -\mathbb{P}_r^{-1} & 0\\ * & * & * & * & -\mathbb{P}_r^{-1}\end{bmatrix}<0 \tag{6}$$

where

$$\mathbb{Q}_r\triangleq-\hat{E}^T\bar{P}_r\hat{E}+Sym\left\{\widetilde{\Lambda}_r\tilde{\Phi}^T\mathbb{A}_r\right\}$$
$$\mathbb{H}_r\triangleq\sqrt{\bar{\mu}(1-\bar{\mu})}\mathbb{C}_r^T$$
$$\mathbb{Z}_r\triangleq\sqrt{\bar{\mu}(1-\bar{\mu})}\mathbb{D}_r^T$$
$$\mathbb{R}_r\triangleq\widetilde{\Lambda}_r\tilde{\Phi}^T\mathbb{B}_r$$
$$\mathbb{P}_r\triangleq\sum_{d\in Y}\pi_{rd}\bar{P}_d$$

Proof: Two non-singular matrices $\tilde{G}$, $\tilde{K}$ are introduced:

$$\tilde{G}^{-T}\bar{P}_r\tilde{G}^{-1}=\begin{bmatrix}\bar{P}_r^1 & \bar{P}_r^2\\ \bar{P}_r^3 & \bar{P}_r^4\end{bmatrix}\qquad \tilde{G}\hat{E}\tilde{K}=\begin{bmatrix}I_{\hat{\kappa}+\epsilon} & 0\\ 0 & 0\end{bmatrix}$$
$$\tilde{K}^T\widetilde{\Lambda}_r=\left[\widetilde{\Lambda}_{11r}^T\ \widetilde{\Lambda}_{12r}^T\right]^T\qquad \tilde{G}^{-T}\tilde{\Phi}=\left[0\ \tilde{\Phi}_1^T\right]^T$$
$$\tilde{G}\mathbb{A}_r\tilde{K}=\begin{bmatrix}\circledast & \circledast\\ \circledast & \mathbb{A}_{4r}\end{bmatrix}.$$

It is easy to derive

$$Sym\left\{\mathbb{A}_r^T\tilde{\Phi}\widetilde{\Lambda}_r^T\right\}-\hat{E}^T\bar{P}_r\hat{E}<0,$$

which implies that

$$\tilde{K}^{-T}\begin{bmatrix}\circledast & \circledast\\ \circledast & Sym\left\{\mathbb{A}_{4r}^T\tilde{\Phi}_1\widetilde{\Lambda}_{12r}^T\right\}\end{bmatrix}\tilde{K}^{-1}<0, \tag{7}$$

Then, we construct the following Lyapunov function:

$$V(\zeta)\triangleq\psi^T(\zeta)\hat{E}^T\bar{P}_r\hat{E}\psi(\zeta).$$

Characterizing $\mathbb{E}\{\Delta V(\zeta)\}\triangleq\mathbb{E}\{V(\zeta+1)-V(\zeta)\}$, and $\xi(\zeta)\triangleq\left[\psi^T(\zeta)\ w^T(\zeta)\right]^T$. According to $\hat{E}^T\tilde{\Phi}=0$, one has $Sym\left\{\psi^T(\zeta+1)\hat{E}^T\tilde{\Phi}\widetilde{\Lambda}_r^T\psi(\zeta)\right\}=0$, the following condition can be obtained

$$\begin{aligned}&\mathbb{E}[\ \Delta V(\zeta)+e^T(\zeta)e(\zeta)-\gamma^2w^T(\zeta)w(\zeta)\\&\quad+Sym\left\{\psi^T(\zeta+1)\hat{E}^T\tilde{\Phi}\widetilde{\Lambda}_r^T\psi(\zeta)\right\}\ ]\\&=\xi^T(\zeta)\Re_r\xi(\zeta)\\&<0.\end{aligned}$$

The condition can be deduced that

$$\mathbb{E}\left\{\Delta V(\zeta)+e^T(\zeta)e(\zeta)\right\}<0. \tag{8}$$

Then, let $\delta\triangleq\inf\{\lambda_{min}(-\Re_r)\}$, this leads to

$$\begin{aligned}\mathbb{E}\{V(\infty)-V(0)\}&=\mathbb{E}\left\{\sum_{\zeta=0}^{\infty}\Delta V(\zeta)\right\}\\&\le\mathbb{E}\left\{\sum_{\zeta=0}^{\infty}\left(-\delta\psi^T(\zeta)\psi(\zeta)\right)\right\}\end{aligned}$$

which means that

$$\begin{aligned}\sum_{\zeta=0}^{\infty}\mathbb{E}\left\{\|\ \psi(\zeta)\ \|^2\right\}&=\mathbb{E}\left\{\sum_{\zeta=0}^{\infty}\left(\psi^T(\zeta)\psi(\zeta)\right)\right\}\\&\le\frac{1}{\delta}\{\mathbb{E}\{V(0)-V(\infty)\}\}\\&<\infty.\end{aligned} \tag{9}$$

Therefore, based on Definition 2, it can be concluded that the system (5) is stochastically admissible.

Letting $\Psi=\mathbb{E}\left\{e^T(\zeta)e(\zeta)-\gamma^2w^T(\zeta)w(\zeta)\right\}$, the following inequality can be obtained

$$\begin{aligned}\Psi&\le\sum_{\zeta=0}^{\infty}\mathbb{E}\left\{\Delta V(\zeta)+e^T(\zeta)e(\zeta)-\gamma^2w^T(\zeta)w(\zeta)\right\}\\&=\sum_{\zeta=0}^{\infty}\mathbb{E}\left\{\xi^T(\zeta)\Re_r\xi(\zeta)\right\}\\&<0\end{aligned}$$

which means

$$\mathbb{E}\left\{\sum_{\zeta=0}^{\infty}e^T(\zeta)e(\zeta)\right\}<\gamma^2\sum_{\zeta=0}^{\infty}w^T(\zeta)w(\zeta).$$

Building upon the prior discussion, it can be deduced that the FES (5) achieves stochastically admissible and simultaneously satisfies the $\mathcal{H}_\infty$ performance index γ.

Theorem 2: For given scalars $\bar\mu \in [0,1]$, $\gamma > 0$, and a matrix $\tilde\Phi = \begin{bmatrix}\Phi \\ 0\end{bmatrix}$ fullfills $\hat E^T\tilde\Phi = 0$, if matrices R_r, K_r, M_r, $\Xi_r = \begin{bmatrix}\Xi_{1r} & b_1\Xi_{2r} \\ \Xi_{3r} & b_2\Xi_{2r}\end{bmatrix}$, $\widetilde\Lambda_r = \begin{bmatrix}\widetilde\Lambda_{1r} & \widetilde\Lambda_{2r}\end{bmatrix}^T$, symmetrical positive definite matrix $\bar P_r \triangleq \begin{bmatrix}\bar P_{11r} & \bar P_{12r} \\ * & \bar P_{22r}\end{bmatrix}$ exist, such that the condition (10) holds for each $r \in Y$:

$$\begin{bmatrix}[\hbar_r]_{11} & [\hbar_r]_{12} & [\hbar_r]_{13} & [\hbar_r]_{14} & [\hbar_r]_{15} \\ * & -\gamma^2 I & 0 & [\hbar_r]_{24} & [\hbar_r]_{25} \\ * & * & -I & 0 & 0 \\ * & * & * & [\hbar_r]_{44} & 0 \\ * & * & * & * & [\hbar_r]_{44}\end{bmatrix} < 0 \quad (10)$$

where

$$[\hbar_r]_{12} \triangleq \begin{bmatrix}\widetilde\Lambda_{1r}^T\Phi^T B_r \\ \widetilde\Lambda_{2r}^T\Phi^T B_r\end{bmatrix}$$
$$[\hbar_r]_{13} \triangleq \begin{bmatrix}Q_r & -M_r^T\end{bmatrix}^T$$
$$[\hbar_r]_{14} \triangleq \begin{bmatrix}A_r\Xi_{1r}^T + b_1\bar\mu C_r^T K_r & A_r\Xi_{3r}^T + b_2\bar\mu C_r^T K_r \\ b_1 R_r & b_2 R_r\end{bmatrix}$$
$$[\hbar_r]_{24} \triangleq \begin{bmatrix}B_r^T\Xi_{1r}^T + b_1\bar\mu D_r^T K_r & B_r^T\Xi_{3r}^T + b_2\bar\mu D_r^T K_r\end{bmatrix}$$
$$[\hbar_r]_{15} \triangleq \begin{bmatrix}b_1\sqrt{\bar\mu(1-\bar\mu)}C_r^T K_r & b_2\sqrt{\bar\mu(1-\bar\mu)}C_r^T K_r \\ 0 & 0\end{bmatrix}$$
$$[\hbar_r]_{25} \triangleq \begin{bmatrix}b_1\sqrt{\bar\mu(1-\bar\mu)}D_r^T K_r & b_2\sqrt{\bar\mu(1-\bar\mu)}D_r^T K_r\end{bmatrix}$$
$$[\hbar_r]_{11} \triangleq \begin{bmatrix}\mathcal{O}_r & -E^T\bar P_{12r} + A_r\Phi\widetilde\Lambda_{2r} \\ * & -Q_{22r\lambda}\end{bmatrix}$$
$$[\hbar_r]_{44} \triangleq \begin{bmatrix}\sum_{d\in Y}\pi_{rd}\bar P_{11r} - \Xi_{1r}^T - \Xi_{1r} & \mathbb{N}_{1r} \\ * & \mathbb{N}_{2r}\end{bmatrix},$$

with

$$\mathcal{O}_r \triangleq -E^T\bar P_{11r}E + Sym\left\{\widetilde\Lambda_{1r}^T\Phi^T A_r\right\}$$
$$\mathbb{N}_{1r} \triangleq \sum_{d\in Y}\pi_{rd}\bar P_{12r} - \Xi_{3r}^T - b_1\Xi_{2r}$$
$$\mathbb{N}_{2r} \triangleq \sum_{d\in Y}\pi_{rd}\bar P_{22r} - b_2\Xi_{2r}^T - b_2\Xi_{2r}$$

Hence, the system (5) is stochastically admissible. Simultaneously, the desired filter gains are designed as follows:

$$A_{fr} = \Xi_{2r}^{-1}R_r^T,\ B_{fr} = \Xi_{2r}^{-1}K_r^T,\ C_{fr} = M_r^T. \quad (11)$$

Proof: Since $(\mathbb{P}_r - \Xi_\lambda)\mathbb{P}_r^{-1}(\mathbb{P}_r - \Xi_\lambda)^T \geq 0$, one has

$$\mathbb{P}_r - \Xi_r^T - \Xi_r + \Xi_r\mathbb{P}_r^{-1}\Xi_r^T \geq 0,$$

which means

$$-\Xi_r\mathbb{P}_r^{-1}\Xi_r^T \leq \mathbb{P}_r - \Xi_r^T - \Xi_r. \quad (12)$$

Define $R_r = A_{fr}^T\Xi_{2\lambda}^T$, $K_r = B_{fr}^T\Xi_{2\lambda}^T$, $M_r = C_{fr}^T$.

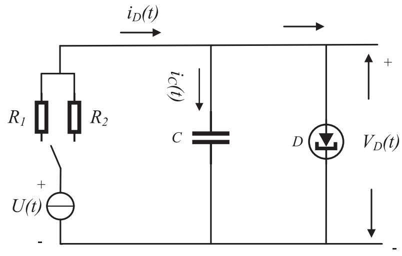

FIGURE 1. Tunnel diode model.

One can obtain from (10) that

$$\begin{bmatrix}\mathcal{O}_r & \widetilde\Lambda_r\tilde\Phi^T\mathbb{B}_r & \Theta_r^T & \mathbb{A}_r^T\Xi_r^T & \mathbb{H}_r\Xi_r^T \\ * & -\gamma^2 I & 0 & \mathbb{B}_r^T\Xi_r^T & \mathbb{Z}_r\Xi_r^T \\ * & * & -I & 0 & 0 \\ * & * & * & -\Xi_r\mathbb{P}_r^{-1}\Xi_r^T & 0 \\ * & * & * & * & -\Xi_r\mathbb{P}_r^{-1}\Xi_r^T\end{bmatrix} < 0 \quad (13)$$

For (13), by multiplying the matrix equation with $\mathrm{diag}\{I, I, I, \Xi_r, \Xi_r\}^{-1}$ and its transpose, the following can be derived by employing the schur complement:

$$\begin{bmatrix}\Psi_{r,\lambda}^1 & \Psi_{r,\lambda}^2 \\ * & \Psi_{r,\lambda}^3\end{bmatrix} < 0,$$

where

$$\Psi_{r,\lambda}^1 = \mathbb{A}_r^T\mathbb{P}_r\mathbb{A}_r + \bar\mu(1-\bar\mu)\mathbb{C}_r^T\mathbb{P}_r\mathbb{C}_r - \hat E^T\bar P_r\hat E + Sym\left\{\widetilde\Lambda_r\tilde\Phi^T\mathbb{A}_r\right\} + \Theta_r^T\Theta_r$$
$$\Psi_{r,\lambda}^2 = \mathbb{A}_r^T\mathbb{P}_r\mathbb{B}_r + \bar\mu(1-\bar\mu)\mathbb{C}_r^T\mathbb{P}_r\mathbb{D}_r + \widetilde\Lambda_r\tilde\Phi^T\mathbb{B}_r$$
$$\Psi_{r,\lambda}^3 = \mathbb{B}_r^T\mathbb{P}_r\mathbb{B}_r + \bar\mu(1-\bar\mu)\mathbb{D}_r^T\mathbb{P}_r\mathbb{D}_r - \gamma^2 I,$$

which is equivalent to (6), this proof is finalized.

IV. A PRACTICAL EXAMPLE

A circuit model includes a tunnel diode is presented in Figure 1 [23]. The parameters within the tunnel diode circuit satisfy the equation $i_d(t) = 0.002u_d(t)$.

Define $x_1(t) = u_d(t)$, $x_2(t) = i_d(t)$, the following equation can be obtained from Kirchhoff's law, and $r \in \{1, 2\}$.

$$\begin{cases} C\dot x_1(t) & = -0.002x_1(t) + x_2(t) \\ 0 & = -x_1(t) - R_r x_2(t) + w(t) \\ y(t) & = C_r x(t) + D_r w(t) \\ z(t) & = Q_r x(t)\end{cases}$$

Additionally, the parameters in circuit is $C = 1.6F$, $R_1 = 1\Omega$, $R_2 = 5\Omega$, the following are the parameters of the system:

$$A_1 = \begin{bmatrix}-0.002 & 1 \\ -1 & -1\end{bmatrix}, A_2 = \begin{bmatrix}-0.002 & 1 \\ -1 & -5\end{bmatrix}.$$

The disturbance input is chosen as $w(\zeta) = \frac{\sqrt{1.66}}{1+\zeta^2}$. Additionally, initial conditions are set as $x(0) = \begin{bmatrix}1.10 & -1.07\end{bmatrix}^T$, and $\tilde x(0) = \begin{bmatrix}0 & 0\end{bmatrix}^T$. In this example, two modes are considered and the specific mode transformation diagram is

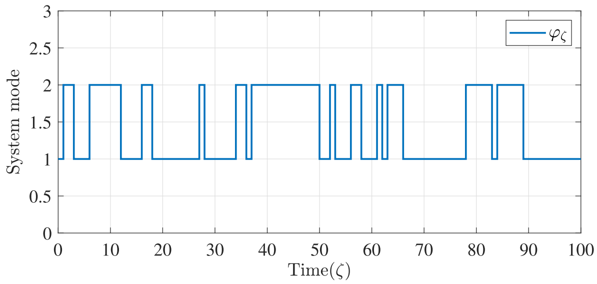

FIGURE 2. Mode evolution.

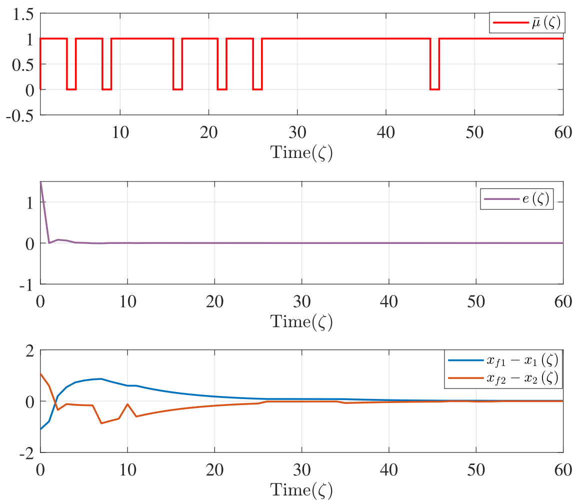

FIGURE 3. Simulation curves when $\bar{\mu} = 0.5$.

shown in Figure 2. Furthermore, we consider three cases of attack probability, which are analysed as follows:

Case 1: If the attack probability $\bar{\mu} = 0.5$:

The filter gains can be calculated from Theorem 2:

$$A_{f1} = \begin{bmatrix} 0.4321 & -0.0042 \\ 0.0035 & -0.0003 \end{bmatrix} \quad B_{f1} = \begin{bmatrix} 0.5231 \\ -0.0113 \end{bmatrix}$$

$$A_{f2} = \begin{bmatrix} 0.4415 & 0.0810 \\ -0.0042 & -0.0016 \end{bmatrix} \quad B_{f2} = \begin{bmatrix} 0.3870 \\ -0.0136 \end{bmatrix}$$

$$C_{f1} = \begin{bmatrix} 1.1871 & 0.0265 \end{bmatrix} \quad C_{f2} = \begin{bmatrix} 1.1051 & 0.2073 \end{bmatrix}$$

The state estimation of the system based on the obtained filter parameters leads to the following simulation curves. Figure 3 plots the sequence diagram of the DoS attack when $\bar{\mu} = 0.5$, the filtering error $e(\zeta)$ and $x_f(\zeta) - x(\zeta)$, respectively.

Case 2: If the attack probability $\bar{\mu} = 0.7$:

Combining with the circuit parameters above, the following filter gains are obtained by solving the linear matrix inequality in Theorem 2:

$$A_{f1} = \begin{bmatrix} 0.2954 & -0.0046 \\ 0.0054 & -0.0003 \end{bmatrix} \quad B_{f1} = \begin{bmatrix} 0.6113 \\ -0.0162 \end{bmatrix}$$

$$A_{f2} = \begin{bmatrix} 0.3619 & 0.0649 \\ 0.0024 & -0.0004 \end{bmatrix} \quad B_{f2} = \begin{bmatrix} 0.4208 \\ -0.0212 \end{bmatrix}$$

$$C_{f1} = \begin{bmatrix} 1.1937 & 0.0085 \end{bmatrix} \quad C_{f2} = \begin{bmatrix} 1.1028 & 0.1982 \end{bmatrix}$$

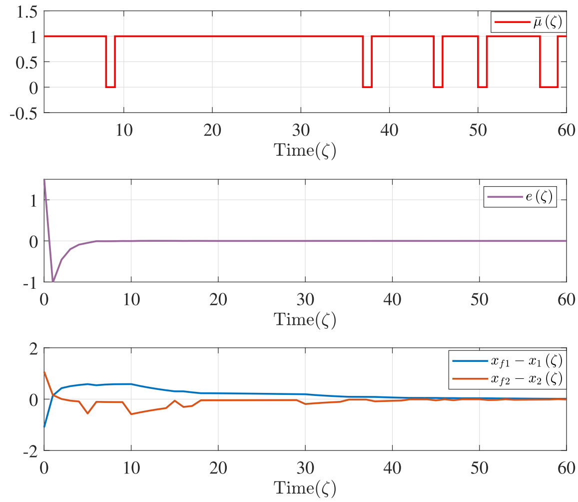

FIGURE 4. Simulation curves when $\bar{\mu} = 0.7$.

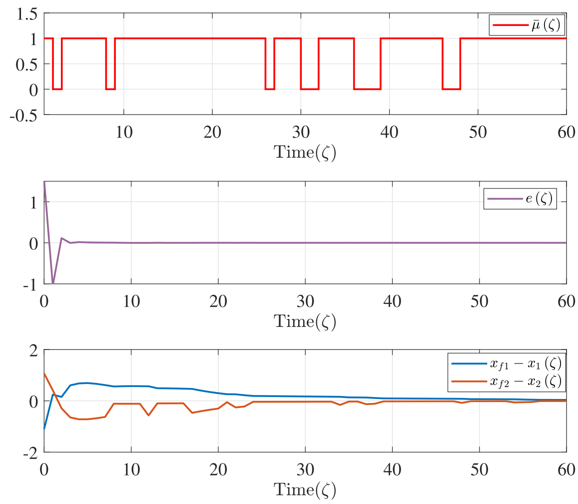

FIGURE 5. Simulation curves when $\bar{\mu} = 0.9$.

Based on the filter parameters obtained above, the following simulation results can also be obtained in Figure 4.

Case 3: If the attack probability $\bar{\mu} = 0.9$:

We can obtain the following filter gains:

$$A_{f1} = \begin{bmatrix} -0.0257 & -0.0012 \\ 0.0387 & 0.0015 \end{bmatrix} \quad B_{f1} = \begin{bmatrix} 0.6796 \\ -0.1200 \end{bmatrix}$$

$$A_{f2} = \begin{bmatrix} 0.1331 & 0.0065 \\ -0.0050 & 0.0005 \end{bmatrix} \quad B_{f2} = \begin{bmatrix} 0.4518 \\ 0.0133 \end{bmatrix}$$

$$C_{f1} = \begin{bmatrix} 1.0198 & 0.0393 \end{bmatrix} \quad C_{f2} = \begin{bmatrix} 0.9295 & 0.0386 \end{bmatrix}$$

The state estimation of the system based on the obtained filter parameters leads to the following simulation curves in Figure 5.

By comparing the simulation results under three different attack probabilities, we can find that the filtering error $e(\zeta)$ shows different simulation effects under different probability of attack, but eventually tend to be stable. This indicates that the filter designed in this paper achieves the expected state estimation effect and the design is effective.

V. CONCLUSION

This paper delves into the $\mathcal{H}_\infty$ filtering of discrete-time SMJSs against DoS attacks, where the DoS attacks follow Bernoulli distribution. Some criteria for regular, causal, and stochastically stability, along with assessing $\mathcal{H}_\infty$ performance of the FES are established. Linear matrix inequalities are employed for filter design, showcasing their feasibility and deriving filter parameters. Finally, a practical example by using a tunnel diode demonstrates the method's efficacy and superiority. Future research should explore nonlinearities in SMJSs and address challenges arising from limited access to state information.

REFERENCES

[1] M. Xu, L. Ma, H. Ma, and Z. Xu, "Sliding mode output feedback controller design of discrete-time Markov jump system based on hidden Markov model approach," *IEEE Access*, vol. 9, pp. 101089–101096, 2021.

[2] P. Cheng, S. He, V. Stojanovic, X. Luan, and F. Liu, "Fuzzy fault detection for Markov jump systems with partly accessible hidden information: An event-triggered approach," *IEEE Trans. Cybern.*, vol. 52, no. 8, pp. 7352–7361, Aug. 2022.

[3] W. Song, B. Li, and J. Zhao, "Hidden mode based controller design for a class of hybrid singular Markovian jump delay systems," *IEEE Access*, vol. 10, pp. 133027–133036, 2022.

[4] A. M. De Oliveira, O. L. V. Costa, G. W. Gabriel, and S. R. Barros Dos Santos, "Energy-to-peak reduced order filtering for continuous-time Markov jump linear systems with partial information on the jump parameter," *IEEE Access*, vol. 10, pp. 79124–79133, 2022.

[5] A. Ahadi, N. Ghadimi, and D. Mirabbasi, "An analytical methodology for assessment of smart monitoring impact on future electric power distribution system reliability," *Complexity*, vol. 21, no. 1, pp. 99–113, 2015.

[6] Y. Feng and X. Gao, "Constrained model predictive control for nonlinear Markov jump system with persistent disturbance via quadratic boundedness," *IEEE Access*, vol. 8, pp. 168273–168281, 2020.

[7] C. Guan, Z. Fei, Z. Feng, and P. Shi, "Stability and stabilization of singular Markovian jump systems by dynamic event-triggered control strategy," *Nonlinear Anal., Hybrid Syst.*, vol. 38, Nov. 2020, Art. no. 100943.

[8] R. Tao, Y. Ma, and C. Wang, "Stochastic admissibility of singular Markov jump systems with time-delay via sliding mode approach," *Appl. Math. Comput.*, vol. 380, Sep. 2020, Art. no. 125282.

[9] Z. Feng and P. Shi, "Sliding mode control of singular stochastic Markov jump systems," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 4266–4273, Aug. 2017.

[10] G. Wang and H. Bo, "Stabilization of singular Markovian jump systems by generally observer-based controllers," *Asian J. Control*, vol. 18, no. 1, pp. 328–339, 2016.

[11] J. Zhao and B. Li, "Finite-time H_∞ robust controller design for a class of singular discrete-time Markov jump delay systems with packet loss compensation and input saturation," *IEEE Access*, vol. 10, pp. 101465–101473, 2022.

[12] J. Wang, D. Wang, L. Su, J. H. Park, and H. Shen, "Dynamic event-triggered H_∞ load frequency control for multi-area power systems subject to hybrid cyber attacks," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 52, no. 12, pp. 7787–7798, Dec. 2022.

[13] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in *Proc. World Congr. Eng.*, 2015, vol. 1, no. 20, pp. 876–3423.

[14] X. Liang and Y. Xiao, "Game theory for network security," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 472–486, 1st Quart., 2013.

[15] G. Xu, H. Li, H. Ren, K. Yang, and R. H. Deng, "Data security issues in deep learning: Attacks, countermeasures, and opportunities," *IEEE Commun. Mag.*, vol. 57, no. 11, pp. 116–122, Nov. 2019.

[16] M. Xing, J. Lu, J. Qiu, and H. Shen, "Synchronization of complex dynamical networks subject to DoS attacks: An improved coding–decoding protocol," *IEEE Trans. Cybern.*, vol. 53, no. 1, pp. 102–113, Jan. 2023.

[17] Y.-W. Wang, Z.-H. Zeng, X.-K. Liu, and Z.-W. Liu, "Input-to-state stability of switched linear systems with unstabilizable modes under DoS attacks," *Automatica*, vol. 146, Dec. 2022, Art. no. 110607.

[18] Y. Pan, Y. Wu, and H.-K. Lam, "Security-based fuzzy control for nonlinear networked control systems with DoS attacks via a resilient event-triggered scheme," *IEEE Trans. Fuzzy Syst.*, vol. 30, no. 10, pp. 4359–4368, Oct. 2022.

[19] W. Gao, C. Deng, Y. Jiang, and Z.-P. Jiang, "Resilient reinforcement learning and robust output regulation under denial-of-service attacks," *Automatica*, vol. 142, Aug. 2022, Art. no. 110366.

[20] H. Shen, M. Xing, Z.-G. Wu, and J. H. Park, "Fault-tolerant control for fuzzy switched singular systems with persistent dwell-time subject to actuator fault," *Fuzzy Sets Syst.*, vol. 392, pp. 60–76, Aug. 2020.

[21] J. Wang, S. Ma, C. Zhang, and M. Fu, "H_∞ state estimation via asynchronous filtering for descriptor Markov jump systems with packet losses," *Signal Process.*, vol. 154, pp. 159–167, Jan. 2019.

[22] Y. Zhang, P. Shi, and S. K. Nguang, "Observer-based finite-time H_∞ control for discrete singular stochastic systems," *Appl. Math. Comput.*, vol. 38, pp. 115–121, Dec. 2014.

[23] S. K. Nguang and W. Assawinchaichote, "H_∞ filtering for fuzzy dynamical systems with D stability constraints," *IEEE Trans. Circuits Syst. I, Fundam. Theory Appl.*, vol. 50, no. 11, pp. 1503–1508, Nov. 2003.

LING CHEN received the M.S. degree in power electronic and electrical drive from Anhui University of Technology, Ma'anshan, China, in 2011. She is currently an Associate Professor with the School of Electrical Information Engineering, Wanjiang University of Technology, Ma'anshan. Her current research interests include power electronics power conversion and optimize control and filtering and their applications.

GUANQI WANG is currently pursuing the M.S. degree with the School of Electrical and Information Engineering, Anhui University of Technology, China. His current research interests include singular systems, Markov jump systems, networked control systems, fuzzy control, robust control, and filtering.

FENG LI received the M.S. degree in electrical engineering from Anhui University of Technology, Ma'anshan, China, in 2017, and the Ph.D. degree in control science and engineering from Nanjing University of Science and Technology, Nanjing, China, in 2021.

He is currently a Lecturer with the School of Electrical and Information Engineering, Anhui University of Technology. From April 2019 to November 2020, he was a Visiting Fellow with the School of Computer, Data and Mathematical Sciences, Western Sydney University, Sydney, NSW, Australia. His current research interests include stochastic hybrid systems, two-time-scale systems, complex networks, networked control systems, fuzzy systems and control, robust control, and filtering and their applications.